Annotated Bibliography

Dual-Use Technologies: Network Traffic Management and Device Intrusion for Targeted Monitoring

By Siena Anstis, Sharly Chan, Adam Senft, and Ronald J. Deibert

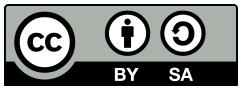
Last Updated: September 2019

THECITIZENLAB

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

Copyright



Citizen Lab engages in research that investigates the intersection of digital technologies, law, and human rights.

Document Version: 1.0

Acknowledgements

Special thanks to Miles Kenyon, Jakub Dalek, and Christopher Parsons. The design of this document is by Mari Zhou.

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a “mixed methods” approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

Contents

Introduction

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a "mixed methods" approach to research combining practices from political science, law, computer science, and area studies. Our research includes: investigating digital espionage against civil society; documenting Internet filtering and other technologies and practices that impact freedom of expression online; analyzing privacy, security, and information controls of popular applications; and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and surveillance activities.

As cybersecurity issues have mounted, dual-use technologies have proliferated. These technologies can be used for legitimate and socially beneficial purposes. However, they can also undermine human rights depending on how they are deployed. For example, network traffic management technology such as deep packet inspection (DPI) and Internet filtering tools can be used legitimately for traffic management. However, they can also be used to undermine human rights by blocking political content or intercepting communications. Malicious software built for "lawful interception," such as zero-day exploits, can lead to human rights abuses if there are improper safeguards or oversight mechanisms in place.

The proliferation of these dual-use technologies stems in part from an increase in private companies who create suites of technology that are ready to be deployed by law enforcement and security agencies, allowing any government to access capabilities that were previously difficult to obtain. This growing appetite for cybersecurity products and services has created a large and growing industry with proven abuse potential.

This annotated bibliography provides a high-level introduction to deep packet inspection, Internet filtering, and targeted intrusion dual-use technologies with the aim of familizaring the reader with their key technical features, the surrounding international human rights law framework, and some of the leading research to date on their deployment. The annotated bibliography also contains a glossary of defined technical terms that should help familiarize the reader with common language in this domain.

Deep Packet Inspection and Internet Filtering

The first category of Citizen Lab research concerns deep packet inspection (DPI) and Internet filtering technologies that private companies can use for traffic management, but which can also be used by Internet service providers (ISPs) to prevent entire populations from accessing politically sensitive information online and/or be used for mass surveillance. This category of research uses a combination of network measurement methods, technical interrogation tests, and other "fingerprinting" techniques to identify the presence on national networks of such technologies capable of surveillance and filtering, and, where possible, the company supplying the technology.

In conducting such research, questions frequently arise regarding the corporate social responsibility practices of the companies developing and selling this technology, as several of Citizen Lab's reports in this area have identified equipment and installations which have been sold by companies to regimes with dubious human rights track records. Citizen Lab's research, described in the annotations below, has spotlighted several companies—namely Blue Coat, Sandvine, and Netsweeper—that provide filtering and DPI systems to such rights-abusing countries.

Commercial-Grade Malware and Spyware

The second category of Citizen Lab research concerns the use of malicious software—"malware"—which is sometimes billed as a tool for lawful intercept. Examples include zero-day exploits and remote access trojans that enable surveillance through a user's device. A zero-day, also known as a 0day, is an undisclosed computer software vulnerability. Zero-days can be considered precious commodities that are traded and sold by black, grey, and legitimate market actors. Law enforcement and intelligence agencies purchase and use zero-days or other malware—typically packaged as part of a suite of "solutions"—to surreptitiously get inside a target's device. When used without proper safeguards, these tools, and the services that go along with them, can lead to significant human rights abuses.

Citizen Lab's work in this area typically begins with a patient zero—someone or some organization that has been targeted with a malware-laden email or link. Over the last few years, Citizen Lab has documented numerous cases, described in the annotations below, of human rights defenders and other civil society groups being targeted with advanced commercial spyware sold by companies like Italy-based Hacking Team, UK/Germany/Swiss-based Finfisher, and Israel-based NSO Group. Using network scanning techniques that employ digital fingerprinting for signatures belonging to the so-called command and control infrastructure used by this malware, Citizen Lab has also been able to map the proliferation of some of these systems to a large and growing global client base, many of which are governments that have a history of human rights abuses.

Citizen Lab's research findings to date only reveal a small part of a much larger problem. The market for dual-use technologies, particularly spyware, is growing rapidly. Government demand for these technologies may actually be increasing following the Snowden disclosures, which raised the bar on

what is deemed *de rigueur* in digital surveillance, and ironically may have intensified competition around the sale of zero-day exploits and methods for defeating increasingly pervasive end-to-end encryption and other defensive measures.

Infringement of Internationally-Accepted Human Rights

The technologies reviewed in this annotated bibliography demonstrate how dual-use technologies have the capability to infringe on internationally-accepted human rights. In this section, we provide a high-level summary of the applicable international human rights legal instruments that are engaged by the manufacture, sale, and deployment of DPI, Internet filtering, and spyware/malware surveillance technologies. As state protections for such fundamental rights vary from jurisdiction to jurisdiction, we have chosen to focus on international frameworks and norms—in particular, the *International Covenant on Civil and Political Rights* (ICCPR) and the *Universal Declaration of Human Rights* (UDHR)—as a starting point for this high-level discussion.

The deleterious human rights impacts of spyware, malware, DPI systems, and Internet filtering technologies have been discussed in detail by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, in multiple reports to the UN. In his 2017 report to the UN Human Rights Council, the Special Rapporteur addressed the role played by private actors engaged in the provision of Internet and telecommunications. He observed that the "multiple uses" of design network equipment and technology raised freedom of expression and privacy concerns. For example, DPI technologies, which could be used for innocuous purposes, "have also been employed to filter Internet content, intercept communications and throttle data flows."

As the Special Rapporteur stated, the improper use of DPI and Internet filtering technologies to mediate publicly-available Internet access by states poses a significant threat to human rights when that filtering is applied covertly, arbitrarily, without due process, or without regard for legitimate forms of expression. The practice of Internet filtering most directly threatens the right to freedom of opinion and expression (UDHR Art. 19, ICCPR Art. 19). This right includes the absolute right "to hold opinions without interference" (ICCPR Art. 19(1)), as well as the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers" whether online or otherwise (ICCPR Art. 19(2)). While freedom of expression is not an absolute right, state restrictions on freedom of expression are subject to strict conditions (ICCPR Art. 19(3)).

The use of malware and spyware in order to engage in targeted surveillance also poses a significant threat to freedom of opinion and expression, particularly in the context of facilitating the targeted surveillance of human rights defenders, civil society activists, and political dissidents. As Special Rapporteur David Kaye noted in his June 2019 report to the UN Human Rights Council, even the threat of surveillance can have chilling effects on people's online activities and can shape and restrict "their capacity to exercise the rights to freedom of expression, association, religious belief, culture and so

forth." As the Special Rapporteur summarized: "In short, interference with privacy through targeted surveillance is designed to repress the exercise of the right to freedom of expression."

Further, technology like DPI systems, Internet filtering technologies, and spyware/malware also impacts the right to privacy (UDHR Art. 12, ICCPR Art. 17). While restrictions on the right to privacy are permissible, such restrictions are subject to strict limitations under international law. Further, given that targeted surveillance disproportionately impacts vulnerable groups, including racial, religious, ethnic, gender, and sexual minorities, state surveillence practices arguably may also violate international human rights prohibitions on discrimination and protections for minority rights (UDHR Art. 7, ICCPR Arts. 26 and Art. 27) and may infringe upon other rights such as the rights to liberty and security of the person (UDHR Art. 3, ICCPR Art. 9).

Annotated Bibliography

This living document provides an introductory reading list and primer on network traffic management and device intrusion for targeted monitoring through key reports and documents. The sources are divided into three themes:

1) Dual-Use Surveillance Technologies and Human Rights
2) Deep Packet Inspection and Internet Content Filtering
3) Commercial-Grade Spyware and Malware

This document is only a snapshot of particular issues with dual-use technologies and targeted monitoring. As such, we have included a list of additional resources that are regularly updated with research and news on targeted monitoring, and litigation in this space.

Dual-Use Surveillance Technologies and Human Rights

What to Do About "Dual Use" Digital Technologies?

Ron Deibert

Deibert, Ron. What to do about "dual use" digital technologies? *Ronald Deibert [Blog],* November 29, 2016. https://deibert.citizenlab.ca/2016/11/dual-use/.

Crux

This written testimony to the Canadian Senate Standing Committee on Human Rights discusses the human rights concerns regarding the sale of dual-use technologies. These technologies may be used for legitimate and beneficial purposes, but also have the capability to surveil users or to censor online information at the country network level. The testimony discusses two categories of Citizen Lab research on dual-use technologies: network traffic management technologies and malicious software. It also provides suggestions to improve the regulation of dual-use technologies.

Highlights

- Network traffic management technologies, such as deep packet inspection (DPI) and Internet filtering tools, can be used legitimately for traffic management. However, they can also be used to undermine human rights by blocking political content or intercepting communications.
- Malicious software built for lawful interception, such as zero-day exploits, can lead to human rights abuses if there are improper safeguards or oversight mechanisms in place.
- Effective solutions that encourage respect for human rights may depend on at least two key components: transparency of the market and creation of an incentive structure to which private sector actors will respond.

Communities @ Risk: Targeted Digital Threats Against Civil Society

Citizen Lab

Citizen Lab. *Communities @ Risk: Targeted Digital Threats Against Civil Society*. Citizen Lab, University of Toronto, November 11, 2014. https://targetedthreats.net/media/1-ExecutiveSummary.pdf.

Crux

The Citizen Lab conducted a multi-year and multi-group study on targeted digital threats, which was defined as persistent attempts to compromise and infiltrate the networked devices and infrastructure

of specific individuals, groups, organizations, and communities. The report involved 10 civil society organizations (CSOs) and provided insight into the impact of targeted digital threats on CSOs.

Highlights

- While the Internet and digital technologies have brought upon many benefits for human rights defenders (HRDs), they also have many risks. For example, governments have been able to exploit the Internet and other digital technologies as tools of mass surveillance for national security and foreign policy aims. There have also been a growing number of case studies and reports of journalists and HRDs being targeted by governments with malicious software (malware) or commercial spyware.
- This report provides a detailed overview of the different types of targeted digital threats and the distinct models that characterize the capacities and tactics of such threat actors. Three are considered here:
    - (1) advanced persistent threats (APTs) characterized by threat actors with the capacity to develop their own resources and conduct wide scale operations;
    - (2) repurposed crimeware (e.g., Remote Access Trojans circulated amongst hobbyists and criminals); and
    - (3) commercial "lawful intercept" products or commercial spyware where private companies offer states turnkey surveillance solutions.
- This report is primarily focused on research that has followed the APTs model with a focus on China-based threat actors targeting CSOs; thus, it has some limitations. However, this research has led to some key findings. For example, targeted digital threats threaten CSOs' core communications and missions in a significant way and extend the reach of repressive state or other non-state actors into perceived safe havens.

Commercial Spyware: The Multibillion Dollar Industry Built on an Ethical and Legal Quagmire

Sarah McKune, Ron Deibert, Bill Marczak, Geoffrey Alexander, and John Scott-Railton

McKune, Sarah, Ron Deibert, Bill Marczak, Geoffrey Alexander, and John Scott-Railton. *Commercial Spyware: The Multibillion Dollar Industry Built on an Ethical and Legal Quagmire*. Citizen Lab, University of Toronto, December 6, 2017.
https://citizenlab.ca/2017/12/legal-overview-ethiopian-dissidents-targeted-spyware/.

Crux

This legal overview and accompaniment to Citizen Lab report, *Champing at the Cyberbit*, highlights the need for clear legal pathways for extraterritorially-targeted individuals to seek recourse against such surveillance. The Ethiopian Government has been targeting civil society actors around the world and conducting extraterritorial surveillance. Governments like Ethiopia have faced little pressure to cease this type of digital targeting.

Highlights

- A 2014 case between an Ethiopian-born American citizen (known under the pseudonym of Kidane) versus the Ethiopian government revealed the lack of remedies for those targeted by extraterritorial surveillance.
- Kidane's computer was infected with FinSpy spyware and alleged that the Ethiopian government had violated the United States *Wiretap Act* when it used FinSpy to infect his computer and engage in ongoing interception, monitoring, and collection of his communications and data.
- The court dismissed the *Kidane v. Ethiopia* case in May 2016, and dismissed Kidane's appeal, concluding that "the *Wiretap Act* does not create a private cause of action against a foreign state and that the plaintiff's state-law tort claim is barred by the *Foreign Sovereign Immunities Act* (FSIA)." Subsequent appeals and petitions were denied.
- The *Kidane v. Ethiopia* dismissal sets a troubling precedent: a foreign government may infect devices and inflict significant harm within the United States on American citizens using digital tools. According to the court's reasoning, digital compromise occurring within the United States does not satisfy the requirements of the *Wiretap Act*. If any intent is formed or any programming occurs abroad, legal remedy is unavailable.
- The Ethiopian government's use of Cyberbit spyware provides a look into the proliferation of commercial spyware companies and its sale of these tools to government entities with track-records of human rights abuses.
- The authors also note how Cyberbit spyware undermines the security of the wider digital ecosystem when they spoof legitimate companies like Adobe Flash Player to deceive targets. There may be grounds for legal action and other remedies by those who were illegitimately targeted or falsely impersonated for trademark misappropriation.
- In sum, there is a need for a comprehensive review of legal, regulatory, and corporate social responsibility measures by governments and the international community.

Advancing Human Rights-by-Design in the Dual-Use Technology Industry

Jon Penney, Sarah McKune, Lex Gill and Ronald Deibert

Penney, Jon, Sarah McKune, Lex Gill, and Ronald J. Deibert. "Advancing Human Rights-by-Design in the Dual-Use Technology Industry." *Columbia Journal of International Affairs* 71, no. 2 (2018): 103-110. https://jia.sipa.columbia.edu/advancing-human-rights-design-dual-use-technology-industry.

Crux

This article summarizes the applicable international human rights law framework in the context of dual-use technology (such as deep packet inspection or spyware) and argues that a "human-rights-by-design" principle is a productive step in ensuring that new dual-use technologies are not used in a way that has a negative human rights impact.

Highlights

- This article provides an overview of the conditions that allow for the proliferation of dual-use technology to be used by authoritarian regimes and applicable principles of international human rights law.
- The authors argue that businesses can do more to mitigate the human rights impact of emerging technologies by adopting a "human-rights-by-design" principle. This principle is defined as committing "to designing tools, technologies, and services to respect human rights by default, rather than permit abuse or exploitation as part of their business model."

The Global Surveillance Industry

Privacy International

Privacy International. *The Global Surveillance Industry*. July 2016. https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.

Crux

This report maps electronic surveillance technologies, the companies that manufacture and export them, and existing regulations governing the trade. It provides a useful typology to categorize different corporate actors involved in surveillance, categorizing 528 surveillance companies (*See Surveillance Industry Index in Additional Resources*).

Highlights

- Electronic surveillance techniques have been central to law enforcement and intelligence agencies since the Cold War. Privacy International notes how the proliferation of these technologies are partly driven by weak regulatory mechanisms, the low cost of these techniques, and technological developments.
- This report describes the different types of technologies that fall within the surveillance industry, including data analysis, audio surveillance, video surveillance, phone monitoring, location monitoring, Internet monitoring, monitoring centres, intrusion equipment, biometrics, counter-surveillance technology, and forensics.
- The report also describes the regulatory mechanisms and trade controls in place to manage the trade of surveillance technologies. In 2012, phone monitoring technology was added to the *Wassenaar Arrangement* list and, in 2013, intrusion software and a provision on Internet monitoring technology were also added.
- The report concludes by saying that safeguards are a matter of urgency in this space and that a comprehensive approach is necessary for incorporating both export restrictions, where possible, and improved standards in corporate social responsibility.

Submission of the Citizen Lab to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on the Surveillance Industry and Human Rights

Siena Anstis, Ron Deibert, and Jon Penney

Anstis, Siena, Ron Deibert, and Jon Penney. *Submission of the Citizen Lab to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on the Surveillance Industry and Human Rights.* Human Rights Council, June 2019. https://citizenlab.ca/wp-content/uploads/2019/02/Submission-to-the-UN-Special-Rapporteur-on-the-promotion-and-protection-of-the-right-to-freedom-of-opinion-and-expression-on-the-surveillance-industry-and-human-rights-2.pdf.

Crux

This Citizen Lab submission to the UN Special Rapporteur uses existing Citizen Lab research to provide an overview of trends of concern within the surveillance industry. For example, there is a lack of transparency and limited national or international measures to hold businesses accountable. It also articulates potential issues to consider in bringing accountability and transparency to this industry.

Highlights

- Common trends among private companies in the surveillance industry include the continued sale of technology to states with poor human rights records, denial of liability for spyware abuses, doing business in violation of fundamental human rights, limited accountability measures, and a non-transparent working environment.
- Going forward, more work is required to describe and identify practices of concern in the spyware industry and develop an accountability framework and take steps towards implementing it. Further, states need to take concrete steps to prevent corporate human rights abuses abroad.

Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression

David Kaye

Kaye, David. *Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.* Human Rights Council, June 2019. https://citizenlab.ca/wp-content/uploads/2019/06/Special-Rapporteur-report-Surveillance-and-human-rights.pdf.

Crux

This Special Rapporteur report to the Human Rights Council provides an overview of the surveillance industry and raises concerns regarding accountability, transparency and the governance of this industry. It also identifies steps required to remedy the human rights concerns that are inherent to the surveillance industry, including, as a first step, a moratorium on the global sale and transfer of the tools of the surveillance industry.

Highlights

- After a review of existing mechanisms for accountability in the surveillance industry, Kaye concluded that the current framework for regulation and accountability was so limited that "an immediate moratorium" was required "on the global sale and transfer of the tools of the private surveillance industry until rigorous human rights safeguards are put in place to regulate such practices and guarantee that Governments and non-State actors use the tools in legitimate ways."
- Below are some of the International Covenant on Civil and Political Rights (ICCPR) articles that apply in the context of the surveillance industry:
    - States are constrained in their ability to infringe on and limit freedom of expression and the right to privacy under the ICCPR. the General Assembly has stated that infringements due to the surveillance of digital communications has to be consistent with international human rights law. It also needs to be "conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory."
    - The UN Human Rights Committee has articulated that the right to privacy in the context of surveillance, interception, and hacking requires "robust, independent oversight systems" that would include ensuring judicial authorization of such measures and effective remedies in cases of abuse.
    - Under Article 2 of the ICCPR, states also have a duty to "protect individuals against third-party interference" and, pursuant to the UN Guiding Principles on Business and Human Rights, states have a "duty to protect" which includes "a duty to take appropriate steps to prevent, investigate, punish and redress human rights abuse by third parties."
- Below are some of the available accountability and regulatory mechanisms that apply—or might apply—to the surveillance industry:
    - **UN Guiding Principles on Business and Human Rights (UNGPs):** Provides a principled framework for human rights compliance by corporate actors and for articulating the duties of States to protect human rights. Moreover, states have a "duty to protect" which includes "a duty to take appropriate steps to prevent, investigate, punish and redress human rights abuse by third parties." There is no mandatory compliance or enforcement mechanisms for UNGPs but they do provide a helpful benchmark for assessing how companies consider human rights compliance.
    - Companies in the surveillance industry have failed to take these norms seriously and implement robust protections for human rights.

- **Export Controls:** The use of export controls to regulate the sale and transfer of surveillance technologies is another mechanism that has been used to exercise greater control over the sale and distribution of surveillance technologies.
    - While there was momentum for greater consideration of the human rights impacts of dual-use technologies in the context of the European *Wassenaar Arrangement*, for example, recent developments have suggested that there is little appetite in the European Union for such reforms.
    - Export control regimes to date have been criticized as imperfect mechanisms in this context. One particular concern is that enforcement of export controls varies from jurisdiction to jurisdiction leading to an inconsistent framework and there are few meaningful effective mechanisms to ensure compliance by companies.
- **Litigation and other types of complaints:** In the past few years, there has been a growth of litigation and the use of other types of complaint mechanisms in the context of the surveillance industry and against both state actors using surveillance technology as well as against corporate actors who manufacture and sell such technology.
    - However, it remains to be seen whether existing actions will be successful and the types of remedies they may lead to.
    - The cost and complexity of litigation is likely a barrier to this avenue becoming a successful mechanism for accountability.
    - The digital nature of the surveillance activities in question raises challenges in attribution, leading to further complexity in the litigation process.
    - Other complaint mechanisms, such as complaints to the Organization for Economic Cooperation and Development, have had limited success.

A Proposed Response to the Commercial Surveillance Emergency

Siena Anstis, Ronald J. Deibert, and John Scott-Railton

Anstis, Siena, Ronald J. Deibert and John Scott-Railton. *A Proposed Response to the Commercial Surveillance Emergency.* Lawfare, July 19, 2019.
https://www.lawfareblog.com/proposed-response-commercial-surveillance-emergency.

Crux

The authors explain how surveillance technology, in particular commercial spyware, has been used to silence dissent and how companies in this industry operate in an industry without restraints. The authors respond to David Kaye's call for a moratorium on the global sale and transfer of the tools of the private surveillance industry.

Highlights

- The authors argue that rigorous human rights safeguards against the surveillance industry, as called for by David Kaye, will require many elements. For example, compliance with the United Nations Guiding Principles on Business and Human Rights; subjecting the purchase and use of surveillance technology by law enforcement or other government bodies to public debate; transparency; and compliance with international frameworks in the use of such technologies.
- The authors argue that the effects of surveillance technology like commercial spyware is becoming more apparent, particularly with a growing number of civil society individuals targeted by authoritarian and repressive regimes.

Rethinking Risk and Security of Human Rights Defenders in the Digital Age

Stephanie Hankey and Daniel O Clunaigh

Hankey, Stephanie, and Daniel O Clunaigh. "Rethinking Risk and Security of Human Rights Defenders in the Digital Age." *Journal of Human Rights Practice* 5, no. 3 (2013): 535-547. https://doi.org/10.1093/jhuman/hut023.

Crux

This article examines how human rights defenders (HRDs) are simultaneously empowered by digital technologies in their advocacy work but can also be vulnerable to new points of weakness. The authors note how digital attacks on HRDs have escalated in the period between 2011-2013 and suggest that a capacity building process is needed for HRDs to be empowered to respond to digital security threats.

Highlights

- The work of HRDs often pose a direct threat to powerful interests who are willing and—all too often—able to constrain or terminate their work. As a result, HRDs and their networks are often the targets of these attacks.
- Digital technologies are used to target HRDs in a few ways: directly monitoring the actions of HRDs and their networks, collecting and using information gathered as evidence against HRDs, entrapment or misinformation, and by blocking and censoring web-based content.
- Hankey et al. also note how there has always been a close link between the role of information in physical threats to HRDs and techniques for psychological intimidation and control. Digital threats are extensions of existing control mechanisms.
- HRDs have unequal access to resources to protect themselves, and when they do use techniques like encryption to protect themselves, they may run the risk of drawing unwanted attention.

Digital Security in Context: Learning how Human Rights Defenders Adopt Digital Security Practices

Becky Kazansky

Kazansky, Becky. *Digital Security in Context: Learning how human rights defenders adopt digital security practices*. Tactical Technology Collective, 2015. https://secresearch.tacticaltech.org/media/pages/pdfs/original/DigitalSecurityInContext.pdf

Crux

This study, conducted over 18 months with over 60 participants, examines the following:
the role of digital security strategies in human rights work and a literature review of related human computer interaction (HCI) and science and technology studies (STS). It also includes findings from three digital security trainings where Kazansky examines the digital security concerns and the formation of digital strategies, as well as any specific challenges around digital security tools and practices in relation to the three trainings.

Highlights

- The researchers found that participants were more aware of surveillance, privacy, and digital security when their peer groups and networks shared stories of security incidents.
- Participants often believed that malware was deployed with the intention of destroying files but rather, targeted malware has been used to monitor and extract sensitive information without destroying them.
- Social engineering is often used to execute malware programs. For example, some attackers will send emails with fake conference invitations that pertain to their interest.
- Corporate platforms like Facebook are difficult for HRDs to protect themselves properly due to the constantly changing Terms of Service and privacy settings.
- Language differences are a barrier for HRDs learning about and applying digital security practices. Translation efforts fail to capture the same meaning – digital security training must be conducted with culturally relevant metaphors and made contextually appropriate.
- Security can be achieved when practised in a collective. There is only so much you can do on an individual level as privacy extends to the people you are connected to.

Social Engineering Attacks on Government Opponents: Target Perspectives

William Marczak and Vern Paxson

Marczak, William, and Vern Paxson. “Social Engineering Attacks on Government Opponents: Target Perspectives.” *Proceedings on Privacy Enhancing Technologies, 2017*, no. 2 (2017): 172–185. https://doi.org/10.1515/popets-2017-0022.

Crux

Repressive nation-states, and other well-resourced attackers, often use social engineering to target activists, NGOs, and civil society for abusive surveillance. Marczak and Paxson conducted 30 interviews with potential targets of Middle Eastern and Horn of Africa-based governments and examined the settings and software of their computers and phones to understand the ways targets can be vulnerable to different types of social engineering techniques.

Highlights

- Surveillance of activists, NGOs, and civil society has moved beyond passive methods and towards hacking devices to retrieve information. This is mainly due to the increased use of encryption, as well as a desire to target those beyond a nation-state's borders.
- This kind of hacking often involves social engineering as a first step to try and get the target to open a malicious artifact like a link or attachment in a message. In some cases, this can involve the use of products or services by commercial lawful interception vendors.
- Interviewees had similar behaviours to ordinary users but they have different perceptions of risk. More than half of the on-the-ground activists feared that surveillance would lead to government punishment.
- Interviewees also used specific security behaviours, such as using out-of-country human password managers to maintain the security of online accounts.
- Interviewees performed basic vetting before opening attachments but their level of checking could still be vulnerable to sender spoofing and doppelganger accounts. This is particularly true if a victim's friend or contact is compromised.
- Marczak and Paxson suggest that a tool supporting automated message checking could benefit CSOs, activists, and NGOs.

A Look at Targeted Attacks Through the Lens of an NGO

Stevens Le Blond, Adina Uritesc, Cédric Gilbert, Zheng Leong Chua, Prateek Saxena, and Engin Kirda

Le Blond, Stevens, Adina Uritesc, Cédric Gilbert, Zheng Leong Chua, Prateek Saxena, and Engin Kirda. "A Look at Targeted Attacks Through the Lense of an NGO." *Proceedings of the 23rd USENIX Security Symposium*, August 20-22, 2014.
https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/le-blond.

Highlights

This paper examines targeted attacks against NGOs that represent the minority Uyghur population in China. Social engineering and using malicious documents is a major component of these targeted threats. Researchers found that the victims, along with their colleagues, were targeted over a course of several years.

Crux

- Le Blond et al. define targeted attacks as low-volume, socially engineered communication which entices specific victims into installing malware. They aim to compromise specific, high-value victims which garners substantial media attention. It is commonly thought that targeted attacks are generally state-sponsored.
- The report found that attackers often used social engineering to target individuals. In this case, the language and topic of malicious email messages were in the mother-tongue of the victims. Emails were highly targeted, referring to specific conferences or events that would only be of interest to the targeted victims.
- In many cases, sender impersonation was common, with some compromised accounts belonging to high-profile activists. Often times, these email addresses would have typos but correspond to the full names of the target's contacts. This means that the attacker had knowledge of the victim's social context.
- The study found that malicious documents were the most popular attack vectors. These attacks tend to use newly released public vulnerabilities, often within a week, and continued to utilize them for several years instead of zero-day vulnerabilities.
- The second most common attack vector in this study was malicious archives like RAR and ZIP files containing malicious executable files.

Deep Packet Inspection and Internet Content Filtering

General

The Politics of Deep Packet Inspection: What Drives Surveillance by Internet Service Providers?

Christopher Parsons

Parsons, Christopher. “The Politics of Deep Packet Inspection: What Drives Surveillance by Internet Service Providers?.” PhD diss., University of Victoria, 2013. https://dspace.library.uvic.ca/bitstream/handle/1828/5024/Parsons_Christopher_PhD_2013.pdf?sequence=6&isAllowed=y.

Crux

This dissertation provides a comprehensive overview of how deep packet inspection (DPI) works, the power structures that exist within the technology themselves, the conditions that drive DPI adoption and governance models, and the privacy implications of DPI.

Highlights

- DPI appliances can be used for private purposes to accomplish the goals of private actors (e.g. network operators can ‘close’ transmissions by informing the applications on peoples’ computers that the transmission has failed).
    - Competitors to internet service providers (ISPs), such as online content providers, said that ISPs would have an interest in discriminating against them.
- DPI appliances can also be used for state surveillance or security purposes and can support lawful access legislation, specifically in intercepting communications (e.g. monitoring for certain kinds of online communications and contents, or by making copies of all data traffic).
    - Civil and consumer rights advocates warned that DPI applications are inherently privacy-invasive because they analyze and act upon the contents of communications. These surveillance practices are normatively inappropriate and often run contrary to national laws that forbid the interception of communications without a warrant.

DPI Technology from the Standpoint of Internet Governance Studies: An Introduction

Milton Mueller

Mueller, Milton. *DPI Technology from the standpoint of Internet governance studies: An introduction.* Syracuse University School of Information Studies, October 21, 2011. https://pdfs.semanticscholar.org/17d8/e798bacba1d93f72d09c03f53857cd62222e.pdf.

Crux

This article examines the main capabilities of deep packet inspection (DPI) and provides a framework of six general use cases of DPIs. Mueller notes how many features of DPI are not new, but rather a complex system that combines new and old techniques and materials (e.g. firewalls and packet capture or packet sniffing techniques). Vendors of DPI technology characterized DPIs as an "enabling technology" where its generic capability can be applied in many use cases or applications.

Highlights

- Capability #1) Recognition involves the detection or identification of things as they move through a network (e.g. detecting protocols, applications, URLs, specific media content, viruses, malware, other exploits, strings of texts, and data that follows specific formats like credit card and social security numbers).
    - Recognition uses pattern analysis to identify digital signatures. These must be predefined and constantly up-to-date. As a result, Mueller notes how "DPI is a service, not just a product, and requires ongoing relationships with signature producers."
- Capability #2) Manipulation involves the "active intervention in a live traffic stream to optimize, control or change it."
    - For example, manipulation can be programmed to block the movement of recognized informational objects into or out of the network, regulate packet flow speed, change the packet header, prioritize or de-prioritize certain protocol packets or a specific user or class of users over others, or disconnect a session.
- Capability #3) Notification capabilities stem from an act of recognition by a DPI appliance. It is a more indirect form of intervention than manipulation.
    - For example, notification can come in the form of statistical reports, alarms or notifications, or generate a billing incident.
- Mueller discerns six groupings of DPI use cases:
    1) **Network visibility and bandwidth management:** Network operators can understand the composition of their traffic.
    2) **User profiling/monetization:** Network operators can use DPI to discriminate ordinary web surfers and those who use Skype or competing services.
    3) **Governmental surveillance (lawful interception):** National laws typically require communications service providers to provide surveillance capabilities or backdoors to government law enforcement or public security agencies. Mueller notes the growing concern of the sale of DPIs to countries with a history of human rights abuses, and the ensuing international debate about export controls in this industry.
    4) **Network security:** Network security was the earliest driver of the development of DPI capabilities. DPI can be used to capture and store information about intrusions, crimes or other suspicious activities.

5) **Copyright policing:** ISPs have been pressured to cooperate in the enforcement of copyright in the context of file sharing.
6) **Content control:** DPI can be used to enforce state censorship by blocking URLs or content with specific keywords or phrases.

Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society

Christian Fuchs

Fuchs, Christian. "Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society". *The Privacy & Security Research Paper Series, Issue #1*, 2012.
http://fuchs.uti.at/wp-content/uploads/DPI.pdf.

Crux

This paper analyzes the societal implications of the use of DPI technologies. The paper reviews product sheets, self-descriptions, and product presentations by 20 European security technology companies that produce and sell DPI technologies. It then considers the societal implications through the review of opinions and reporting by security industry representatives, privacy advocates, and scholars.

Highlights

- DPI capabilities used for one purpose can "function-creep" to other functions that are more privacy sensitive. For example, using DPI for network management or spam filtering but also for targeted advertising or content monitoring for political purposes, law enforcement or the violation of net neutrality.
- Fuchs notes how "DPI can be used for the monitoring of specific users or a large number of users in order to find out with whom they communicate about what, including the content of communication and the filtering of content for keywords."
- The report includes an analysis of various companies reportedly involved in the export of dual-use technologies (for example, Area Spa (Italy), Gamma Group (UK), and Amesys (France)).
- The paper summarizes the potential detrimental effects of DPI technologies when deployed for Internet surveillance, including total internet surveillance, surveillance creep, targeted advertising, surveillance of file sharers, and political repression and social discrimination. The author also notes how "not much is known about the selling and export of communications surveillance technologies" and that there is a "lack of transparency and accountability."
- DPI surveillance shows that understanding new surveillance technologies requires more than just privacy and data protection assessments, but "broader societal impact assessments that are guided by ethics and connected to the analysis of power structures in society.

Blue Coat Systems

Planet Blue Coat: Mapping Global Censorship and Surveillance Tools

Morgan Marquis-Boire, Jakub Dalek, Sarah McKune, Matthew Carrieri, Masashi Crete-Nishihata, Ron Deibert, Saad Omar Khan, Helmi Noman, John Scott-Railton, and Greg Wiseman

Marquis-Boire, Morgan, Jakub Dalek, Sarah McKune, Matthew Carrieri, Masashi Crete-Nishihata, Ron Deibert, Saad Omar Khan, Helmi Noman, John Scott-Railton, and Greg Wiseman. *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools.* Citizen Lab, University of Toronto, January 2013. https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/.

Crux

This report outlines Citizen Lab's investigation into the global use of Blue Coat devices that are capable of Internet filtering, censorship, and surveillance. The investigation identified specific technology being used on public or government networks in countries with a history of human rights concerns, providing a closer look at dual-use information and communication technologies [Note: Blue Coat was acquired by Symantec in 2016.]

Highlights

- Blue Coat Systems has a history of selling their products to countries with known human rights abuses. In 2011, researchers found evidence that these products were being used in Syria. Initially, Blue Coat denied that they sold their equipment to Syria but later admitted that thirteen devices were active in Syria. They subsequently suspended support for these devices, but noted how they do not have a kill switch to remotely disable the devices.
- In order to uncover the global spread of such devices, Citizen Lab scans uncovered 61 Blue Coat ProxySG devices and 316 Blue Coat PacketShaper appliances. There were 61 appliances found in countries with a history of human rights concerns:
    - Blue Coat ProxySG categorizes web pages to permit filtering of unwanted content. It was found in the following countries: Egypt, Kuwait, Qatar, Saudi Arabia, and the UAE.
    - PacketShaper is a cloud-based network management device that can establish visibility of over 600 web applications and control undesirable traffic. It was found in the following countries: Afghanistan, Bahrain, China, India, Indonesia, Iraq, Kenya, Kuwait, Lebanon, Malaysia, Nigeria, Qatar, Russia, Saudi Arabia, South Korea, Singapore, Thailand, Turkey, and Venezuela.
- While these web filtering and network management technologies can be used to improve networks, the sale of such technology may negatively impact human rights in certain cases.
- Citizen Lab uses this research to explore how a combination of methods to address dual-use technology is needed to address the proliferation of such technology. This includes export

control frameworks, corporate social responsibility measures, and self-regulation for companies with frameworks like due diligence processes.

Netsweeper

Tender Confirmed, Rights At Risk: Verifying Netsweeper in Bahrain

Jakub Dalek, Ron Deibert, Bill Marczak, Sarah McKune, Helmi Noman, Irene Poetranto, and Adam Senft

Dalek, Jakub, Ron Deibert, Bill Marczak, Sarah McKune, Helmi Noman, Irene Poetranto, and Adam Senft. *Tender Confirmed, Rights At Risk: Verifying Netsweeper in Bahrain*. Citizen Lab, University of Toronto, September 2016.
https://citizenlab.ca/2016/09/tender-confirmed-rights-risk-verifying-netsweeper-bahrain/.

Crux

This 2016 Citizen Lab report examines Netsweeper's accepted public tender of filtering technology in Bahrain, a country with a history of human rights concerns. The report was published against the backdrop of the Canadian Government's intention to expand ties with the Gulf Cooperation Council (GCC), a regional intergovernmental partnership involving Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the UAE.

Highlights

- Netsweeper, Inc. is a privately-owned technology company based in Waterloo, Ontario, Canada, whose primary offering is an Internet content filtering product and service. They have a range of customers from educational institutions to ISPs and telecommunications companies. Since the public tender was accepted in January 2016 to provide a "National website filtering solution" for Bahrain, Netsweeper installations were active between May-July 2016.
- Citizen Lab found that Netsweeper technology was being used by at least one key Bahraini Internet service provider, Batelco, to filter content including critical political speech, news websites, human rights content, websites of oppositional political groups, and Shia-related content in Bahrain.
- The report raises questions about the corporate social responsibility of Netsweeper Inc., as well as the role of the Canadian Government to regulate the export of these dual-use technologies.

Planet Netsweeper

Jakub Dalek, Lex Gill, Bill Marczak, Sarah McKune, Naser Noor, Joshua Oliver, Jon Penney, Adam Senft, and Ron Deibert

Dalek, Jakub, Lex Gill, Bill Marczak, Sarah McKune, Naser Noor, Joshua Oliver, Jon Penney, Adam Senft, and Ron Deibert. *Planet Netsweeper: Executive Summary.* Citizen Lab, University of Toronto, April 2018. https://citizenlab.ca/2018/04/planet-netsweeper/.

Crux

This Citizen Lab report examines the global use of Internet filtering systems manufactured by Canadian company Netsweeper, Inc. A case study of ten countries revealed how Netsweeper technology was being used to block access to a wide range of digital content protected by international legal frameworks, including religious content, political campaigns, and media websites.

Highlights

- Netsweeper has a pattern of mischaracterization and/or over blocking for keywords related to LGBTQ identities and non-pornographic websites that may have serious human rights implications.
- The "Alternative Lifestyles" category in Netsweeper's filtering disproportionately blocks non-pornographic LGBTQ content and could be configured to block access to websites from entire specified countries. [Note that in a statement to Motherboard, Lou Erdelyi from Netsweeper's chief technology office said "As of December 25th, 2018, Netsweeper no longer has a category titled LGBTQ+ nor does it block such content."]
- The international use of a Canadian-made Internet filtering technology raises questions about human rights, corporate social responsibility, and public policy concerns and questions. These findings raise questions about the due diligence for Netsweeper and the role of the Canadian government in these sales.

Sandvine

Bad Traffic: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?

Bill Marczak, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, and Ron Deibert

Marczak, Bill, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, and Ron Deibert. *Bad Traffic: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?.* Citizen Lab, University of Toronto, March 2018. https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/.

Crux

This Citizen Lab report examines Sandvine's PacketLogic DPI middleboxes that can prioritize, degrade, block, inject, and log various types of Internet traffic. Through their analysis, the Citizen Lab uncovers how Sandvine DPI devices are used to deliver nation-state malware in Turkey and indirectly into Syria, and to covertly raise money through affiliate ads and cryptocurrency mining in Egypt.

Highlights

- DPI middleboxes were found on Türk Telekom's network. They were being used to redirect hundreds of users in Turkey and Syria to nation-state spyware when users attempted to download certain legitimate Windows applications.
- Middleboxes were also found at a Telecom Egypt demarcation point (the physical point where a public network ends and the customer's private network begins) to hijack unencrypted web connections en masse, and redirect them to revenue generating content like ads and browser cryptocurrency mining scripts.
- Dual-use technologies, such as Sandvine's middleboxes, remain unregulated. Existing international mechanisms, such as the *Wassenaar Arrangement* and the *UN Guiding Principles on Business and Human Rights* are non-binding and have been ineffective to regulate the industry to date.

Commercial-Grade Spyware and Malware

Gamma Group/ FinFisher GmbH – FinSpy

From Bahrain With Love: FinFisher's Spy Kit Exposed?

Morgan Marquis-Boire and Bill Marczak

Marquis-Boise, Morgan and Bill Marczak. *From Bahrain with Love: FinFisher's Spy Kit Exposed?*. Citizen Lab, University of Toronto, July 25, 2012.
https://citizenlab.ca/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/.

Crux

The FinFisher Suite has been described as a governmental IT intrusion and remote monitoring solution. The toolset first gained notoriety after it was revealed that the Egyptian government's state security had been involved in negotiations with Gamma International UK Ltd. over the purchase of the software. This report analyzes several pieces of malware that were sent to Bahraini pro-democracy activists in April and May 2012 with the goal of identifying and classifying the malware to better understand the actors behind the attacks and the risk to victims.

Highlights

- This report provides an analysis of how the malware was sent to pro-democracy activists and how it infected their devices. It also discusses how the malware avoids detection and what types of data are collected.
- Citizen Lab's analysis of the malware showed that it collected a wide range of data from an infected victim. The data was stored locally in a hidden directory that was then disguised with encryption prior to exfiltration.
- Files in the hidden directory included screenshots, keylogger data, audio from Skype calls, passwords, and more. The malware tried to locate the configuration and password store files for a variety of browsers and chat clients.
- Citizen Lab's analysis of the malware also showed that it connected to a server owned by Batelco, the principal telecommunications company in Bahrain, and traffic was observed between the infected victim and the command and control host in Bahrain for nearly ten minutes.

The SmartPhone Who Loved Me: FinFisher Goes Mobile?

Morgan Marquis-Boire, Bill Marczak, and Claudio Guarnieri

Marquis-Boire, Morgan and Bill Marczak, and Claudio Guarnieri. *The SmartPhone Who Loved Me: FinFisher Goes Mobile?*. Citizen Lab, University of Toronto, August 29, 2012. https://citizenlab.ca/wp-content/uploads/2015/03/The-SmartPhone-Who-Loved-Me-FinFisher-Goes-Mobile.pdf.

Crux

This report analyzes several samples that appeared to be mobile versions of the FinFisher Toolkit. It also details ongoing Internet scanning that has identified more apparent FinFisher command and control servers in Bahrain, Brunei, the Czech Republic, Ethiopia, Indonesia, Mongolia, Singapore, the Netherlands, Turkmenistan, and the United Arab Emirates.

Highlights

- This report analyzed malware samples that were used to identify apparent mobile Trojans for the iOS, Android, BlackBerry, Windows Mobile, and Symbian platforms. The tools were consistent with the functionality claims regarding FinSpy's mobile product, a component of the FinFisher toolkit.
- This report also describes the scanning of IP addresses in several countries looking for FinSpy command and control servers. The scanning yielded additional countries where command and control servers were operating: Brunei, a server in Turkmenistan's Ministry of Communications, two in Singapore, one in the Netherlands, a new server in Indonesia, and a new server in Bahrain. The scanning technique was also able to confirm the existence of servers in ten countries previously reported by Rapid7.

You Only Click Twice: FinFisher's Global Proliferation

Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton

Marquis-Boire, Morgan, Bill Marczak, Claudio Guarnieri, and John Scott-Railton. *You Only Click Twice: FinFisher's Global Proliferation*. Citizen Lab, University of Toronto, March 13, 2013. https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

Crux

This report highlights the results from a comprehensive global Internet scan for the command and control servers of FinFisher's surveillance software and the discovery of a campaign using FinFisher in Ethiopia to target opposition members. After publishing the first FinFisher report, described above, researchers began to search for other command and control servers to understand how widely FinFisher was being deployed by using different fingerprinting techniques. This report summarizes the findings of that research, and also considers an Android sample of FinSpy Mobile that was found in the

course of the study. It appears to have been used in Vietnam. Despite this body of research, Gamma Group has denied links to the identified spyware and servers.

Highlights

- Internet scanning with new fingerprints identified a total of 36 FinSpy servers, 30 of which were new and six which had been located during previous scanning. The servers were operating in a total of 19 countries, including seven countries not seen before (Canada, Bangladesh, India, Malaysia, Mexico, Serbia, and Vietnam).
- In addition to Internet scanning, this report analyzed a malware sample identified as FinSpy. The malware used images of members of Ginbot7, an Ethiopian opposition group, as bait and communicated with a FinSpy command and control server in Ethiopia. These factors strongly suggest that the Ethiopian government was using FinSpy.
- This report also reviews a malware sample identified as FinSpy Mobile for Android. The FinFisher suite includes mobile phone versions of FinSpy for all major platforms and its features are similar to the computer version but also contains mobile-specific features such as GPS tracking and functionality for silent 'spy' calls to snoop on conversations near the phone.
- The number of FinFisher command and control servers identified through Internet scanning is "indicative of a global trend towards the acquisition of offensive cyber-capabilities by non-democratic regimes from commercial Western companies."

Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation

Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune

Marczak, Bill, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune. *Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation.* Citizen Lab, University of Toronto, October 15, 2015.
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/.

Crux

This Citizen Lab report describes how Internet scanning was used to identify the users of FinFisher, a sophisticated and user-friendly spyware suite sold exclusively to governments. Using a methodology to distinguish between anonymizing proxies and FinSpy master servers, Citizen Lab was able to determine the location of the FinFisher client. The results of this methodology was a total of 33 government users identified as likely users of FinFisher in 32 countries based on the presence of a FinFisher master at an IP address in a country or belonging to a specific government department. This was achieved by correlating scanning results with public sources.

Highlights

- FinFisher is a sophisticated computer spyware suite written by Munich-based FinFisher GmbH and sold exclusively to government law enforcement and intelligence. While marked for fighting crime, the spyware has been involved in a number of high-profile surveillance abuses and has recently been implicated in litigation regarding these abuses.
- Between 2010 and 2012, Bahrain's government used FinFisher to monitor some of the country's top law firms, journalists, activists, and opposition political leaders. Ethiopian dissidents in exile in the United Kingdom and the United States have also been infected with FinFisher spyware.
- Likely FinFisher users included Angola, the Directorate General of Forces Intelligence in Bangladesh, the Belgian Federal Police, the Technology Research Department in Egypt, Ethiopia, Italy, the National Intelligence Service in Kenya, Saudi Arabia, Venezuela, and others.

New FinSpy iOS and Android Implants Revealed ITW

GReAT and AMR

GReAT and AMR. *New FinSpy iOS and Android implants revealed ITW.* Kaspersky, July 10, 2019. https://securelist.com/new-finspy-ios-and-android-implants-revealed-itw/91685/.

Crux

This report by Kaspersky Lab researchers reveals new functionalities of Gamma Group's FinSpy. Mobile intrusions for iOS and Android now have almost the same functionality. According to their research, several dozen unique mobile devices have been infected between 2018-2019 with recent activity recorded in Myanmar in June 2019.

Highlights

- FinSpy is capable of collecting and exfiltrating personal information such as contacts, SMS/MMS messages, emails, calendars, GPS location, photos, files in memory, phone call recordings, and data from the most popular messengers.
- FinSpy for iOS is able to monitor almost all device activities, including WhatsApp and Signal. The implant can only be installed on jailbroken devices (iPhone or iPad) and at the time of the report, an attacker using the main infection vector could only install the implant if they had physical access to the device to jailbreak it. If an iOS device is jailbroken, there are at least three possible infection vectors: SMS message, email, and WAP Push.
- FinSpy for Android is similar to the iOS version, but it is also capable of gaining root privileges (complete access to all files and commands) on an unrooted device (not jailbroken). With more available settings, operators can tailor the behavior of the implant for every victim. FinSpy can be installed manually if the attacker has physical access to the device, and by the following remote infection vectors: SMS messages, emails, and WAP Push.
- Up-to-date versions of these implants were detected in almost 20 countries but given Gamma's customer base, there are likely more victims.

Hacking Team – Remote Control System (RCS)

Hacking Team and the Targeting of Ethiopian Journalists

Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton

Marczak, Bill, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton. *Hacking Team and the Targeting of Ethiopian Journalists*. Citizen Lab, February 12, 2014. https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists/.

Crux

This Citizen Lab report is the first of three reports documenting the global proliferation and use of Hacking Team's Remote Control System (RCS) spyware, which is allegedly sold exclusively to governments. The Citizen Lab reported how the Milan-based Hacking Team's RCS spyware was used to target the Ethiopian Satellite Television Service (ESAT), an independent satellite television, radio, and online news media outlet run by members of the Ethiopian diaspora. The malware communicated with an IP address belonging to Ariave Satcom, a satellite provider that services Africa, Europe, and Asia.

Highlights

- ESAT broadcasts are frequently critical of the Ethiopian government. Their broadcasts have been jammed from within Ethiopia several times over the years.
- The Committee to Protect Journalists (CPJ) reports that Ethiopia jails more journalists than any other African country besides Eritrea, and says that the Ethiopian government has shut down more than seventy-five media outlets since 1993.
- In the space of two hours on December 20, 2013, an attacker made three separate attempts to target two Washington-based ESAT employees with Hacking Team's RCS.
    - RCS is a trojan sold exclusively to intelligence and law enforcement agencies. It works by infecting a target's computer or mobile phone to intercept data before it is encrypted, and it can also intercept data that is never transmitted. RCS can copy files from a hard disk, record Skype calls, emails, instant messages, and passwords typed into a web browser. It can also turn on a device's webcam and microphone.
    - Hacking Team was in the public spotlight in 2012 when RCS was used against award-winning Moroccan media outlet Mamfakinch and United Arab Emirates (UAE) human rights activist Ahmed Mansoor.
- At the time of publication, Hacking Team stated how "they do not sell RCS to "repressive regimes,"" and that RCS is not sold through "independent agents." They also noted how all their sales are reviewed by a board that includes external engineers and lawyers. The board has veto power over any sale. Before authorizing a sale, Hacking Team said that it considers

whether a country would use surveillance technologies to facilitate human rights abuses, as well as "due process requirements" for surveillance.
- This case demonstrates a broader pattern of government abuse of lawful intercept spyware. It also raises questions about whether more mechanisms are needed to regulate the use, sale, and development of commercial spyware and dual-use technologies.

Mapping Hacking Team's Untraceable Spyware

Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton

Marczak, Bill, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton. *Mapping Hacking Team's Untraceable Spyware*, Citizen Lab, February 17, 2014. https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/.

Crux

This Citizen Lab report is the second of three reports documenting the global proliferation and use of Hacking Team's Remote Control System (RCS) spyware, which is sold exclusively to governments. It focuses on how networks of proxy servers are used to launder data that RCS exfiltrates from infected computers (it is roughly analogous to general-purpose anonymity solutions like Tor). This is designed to obscure the identity of the government conducting the spyware.

Highlights

- Networks of proxy servers launder exfiltrated data. The data goes through third countries and to an endpoint, which the Lab believes represents the spyware's government operator. Designed to obscure the identity of the government, Hacking Team advertises that the RCS "collection infrastructure" renders the spyware "untraceable."
    - For example: data destined for an endpoint in Mexico appears to be routed through four different proxies, each in a different country.
- Citizen Lab was able to map out the chain and endpoints through fingerprinting for RCS servers. This is done by observing distinctive current and previous behaviour of servers through historical scanning.
- In order for a government to receive data, they need to infect one or more target devices with the RCS spyware. This can be in the form of:
    - Phishing attacks to convince a user to open or install a disguised file or application.
    - Exploits, which take advantage of bugs in computer software, typically require less user interaction before a successful infection.
- The investigation pointed to 21 suspected government users of RCS, based on the endpoints in the proxy chain and noted five countries of concern: Azerbaijan, Kazakhstan, Uzbekistan, Saudi Arabia, and Sudan.
- These findings demonstrate the dangers of an unregulated marketplace. Despite claiming due diligence, Hacking Team RCS was found in countries with human rights abuses. It also

highlights the professional alignment between exploit sellers, the companies that sell surveillance trojans, and the governments that purchase them for a one-stop-shop.

Hacking Team's US Nexus

Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, John Scott-Railton, and Sarah McKune

Marczak, Bill, Claudio Guarnieri, Morgan Marquis-Boire, John Scott-Railton, and Sarah McKune. *Hacking Team's US Nexus*. Citizen Lab, February 28, 2014. https://citizenlab.org/2014/02/hacking-teams-us-nexus/.

Crux

This Citizen Lab report is the final of three reports documenting the global proliferation and use of Hacking Team's Remote Control System (RCS) spyware, which is sold exclusively to governments. This report reveals the involvement of dedicated US hosting companies in Hacking Team's "collection infrastructure" and its legal implications of being a third-country proxy server.

Highlights

- There are ten foreign governments using RCS proxy chains with a US nexus: Azerbaijan, Colombia, Ethiopia, Korea, Mexico, Morocco, Poland, Thailand, Uzbekistan, and UAE.
- The US receives a lot of global Internet traffic but routing wiretapped data to foreign governments from the US deserves legal scrutiny. Does this violate the US Computer Fraud and Abuse Act and the US Wiretap Act?
    - Foreign governments are not likely asking for permission from the US government to engage in surveillance of US-based targets or to transmit surveilled data.
    - As a result, foreign governments using the RCS spyware in this manner wilfully flout the international legal principles of sovereignty and nonintervention.
- Hacking Team's use of US-based service providers creates liabilities for these companies. These companies would want to follow corporate social responsibility and ensure that their services would not violate US and international law.
- Citizen Lab suspects that Hacking Team did not inform these US-based companies of the nature of the data they transmit.

[Note: Hacking Team had a data breach in 2015, revealing internal documents, emails, and source code of their products. In April 2019, Swiss-Italian company InTheCyber announced that it had acquired a majority stake into Hacking Team, and that it was merging the two companies into a new one called Memento Labs.]

NSO Group – Pegasus

The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against a UAE Human Rights Defender

Bill Marczak and John Scott-Railton

Marczak, Bill and John Scott-Railton. *The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against a UAE Human Rights Defender.* Citizen Lab, University of Toronto, August 24, 2016. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

Crux

This Citizen Lab report describes how Ahmed Mansoor, a human rights defender in the United Arab Emirates, was targeted with NSO Group's Pegasus spyware. Mansoor received text messages with links that were determined to lead to a chain of zero-day exploits (named "Trident" by the researchers) that would have remotely jailbroken Mansoor's iPhone 6 and installed spyware. His phone would have become a spy in his pocket, capable of using his iPhone camera and microphone, recording WhatsApp and Viber calls, loggings messages sent in mobile chat apps, and tracking movement.

Highlights

- This report demonstrates that not all state-sponsored spyware campaigns utilise "just enough" technical means coupled with carefully planned deception, as previous Citizen Lab research had shown. Exploits, such as the one used in this case, are rare, expensive, and technically sophisticated.
- The likely operator behind this targeting was the UAE in light of the high cost of the exploit at issue, the use of a tool sold exclusively to governments, and prior targeting of Mansoor by the UAE. Mansoor had also been targeted with Hacking Team and FinFisher spyware.
- According to documents in the Hacking Team materials, NSO Group offers two remote installation vectors for spyware onto a device: zero-click or one-click vectors.
- A malicious website called an Anonymizer communicates with a Pegasus Installation Server located on the operator's premises. When the target visits a malicious link on their device, the Anonymizer forwards the request to the Pegasus Installation Server, which examines the device's User-Agent header to determine if Pegasus has an exploit chain, such as "Trident," that supports the device. If supported, the server returns the exploit to the target device through the Anonymizer and attempts infection; if the infection fails the target's web browser will redirect to a legitimate website.
- The spyware used against Mansoor confirmed a number of the spyware capabilities advertised in NSO Group documentation. Namely, researchers observed indications that the collection of the following types of data was supported: calls made by phone, WhatsApp, and Viber; SMS message and messages/other data from other applications like Gmail, WhatsApp, and Skype;

and a wide range of personal data such as calendar data and contact lists and passwords (including WiFi).
- This report also sets out how a prior investigation by Citizen Lab into the mobile attack infrastructure of a threat actor named "Stealth Falcon," who was targeting individuals critical of the UAE government at home and abroad, was linked to NSO Group.
- Researchers linked a number of IPs and domain names to what appeared to be the NSO Group exploit infrastructure. These domain names were coded and several common themes were identified. The most common theme was the use of news media in an attempt to get targets to click on spyware links. Two domain names tried to masquerade as an official site of the International Committee of the Red Cross.

Reckless Reports: Abuse of NSO Group's Pegasus Spyware in Mexico (Series)

Various authors

For a complete link to all reports: https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/

Crux

This series of reports describes how numerous human rights defenders and civil society actors in Mexico were targeted with NSO Group's Pegasus spyware. The targets received malicious links that would have installed NSO Group's Pegasus spyware on their phones.

Highlights

- The first report in this series describes how an espionage operation using government-exclusive spyware to target a Mexican government food scientist and two public health advocates. All targets were supporting a public health measure: Mexico's soda tax on sugary drinks. The operation used NSO Group spyware: the messages received by the targets all pointed to domains previously identified as part of the Citizen Lab's investigation into NSO Group's infrastructure. Circumstantial evidence led to the conclusion that there was a strong possibility that the Mexican government participated in the operation.
- Since this first report on targeting in Mexico was published in 2017, a total of 25 individuals have been identified as having been targeted with Pegasus malware in Mexico. These findings are laid out in a subsequent seven Citizen Lab reports. Targets included Mexican journalists, lawyers, and a minor child, senior Mexican legislators and politicians, the director of a Mexican anti-corruption group, and the wife of a journalist slain in a cartel-linked killing.

NSO Group Infrastructure Linked to Targeting of Amnesty International and Saudi Dissident

Bill Marczak, John Scott-Railton, and Ron Deibert

Marczak, Bill, John Scott-Railton, and Ron Deibert. *NSO Group Infrastructure Linked to Targeting of Amnesty International and Saudi Dissident.* Citizen Lab, University of Toronto, July 31, 2018. https://citizenlab.ca/2018/07/nso-spyware-targeting-amnesty-international/.

Crux

The Citizen Lab corroborates Amnesty International's conclusion that one of Amnesty International's researchers, as well as a Saudi activist based abroad, were targeted with NSO Group Pegasus spyware.

Highlights

- Amnesty International shared SMS and WhatsApp messages received by the targets with the Citizen Lab. The domain names in the messages appeared to be part of NSO Group's infrastructure, which was put into place after the Citizen Lab's initial reporting on the company in August 2016. The report concludes that if the targets had clicked on the links, their phones would likely have been infected with NSO Group's Pegasus spyware.
- This report also provides a review of Citizen Lab's findings regarding how the NSO Group infrastructure works based on leaked NSO Group Pegasus documentation and prior reporting on NSO Group by Citizen Lab.

Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries

Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert

Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*. Citizen Lab, University of Toronto, September 18, 2018. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

Crux

This report by the Citizen Lab uncovers how NSO Group's Pegasus Spyware has been used in at least 45 countries. Within a two year period between August 2016-August 2018, the Citizen Lab used Internet scanning to find fingerprints and domain names that matched with NSO Group's Pegasus spyware. Out of the 45 countries identified, at least ten Pegasus operators appeared to be actively engaged in cross-border surveillance. The Citizen Lab also found suspected NSO Pegasus infections associated with 33 of the 36 Pegasus operators. These findings paint a bleak picture of the human rights risks of NSO Group's global proliferation – Pegasus is being used by countries with poor human rights records. Moreover, the Citizen Lab found evidence of possible political themes within targeting materials in several countries, calling into question the legitimacy of criminal investigations that use Pegasus.

Highlights

- The Citizen Lab developed and used a novel technique (named *Athena* by the researchers) to cluster their fingerprint and domain matches into 36 distinct Pegasus systems, each one which appears to be run by a separate operator.
- The Pegasus mobile phone spyware suite is produced and sold by Israel-based cyber warfare vendor, NSO Group. Pegasus customers can infect phones by sending their targets specially crafted exploit links. Once a phone is infected and Pegasus is installed, it begins contacting the operator's command and control (C&C) servers to receive and execute operators' commands. The customer has full access to a victim's files and can have access to the microphone and camera to eavesdrop.
- Pegasus exploit links and C&C servers use HTTPS, which requires operators to register and maintain domain names. These domain names for exploits often look benign at first glance because they impersonate legitimate services.

The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil

Bill Marczak, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, and Ron Deibert

Marczak, Bill, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, and Ron Deibert. *The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil*. Citizen Lab, University of Toronto, October 1, 2018.
https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/.

Crux

This Citizen Lab report examines the case of Saudi dissident and Canadian permanent resident, Omar Abdulaziz. He was targeted with a fake mail package delivery notification. The Citizen Lab attributes this infection, with a high degree of confidence, to a Saudi operator of NSO Group's Pegasus spyware.

Highlights

- Omar Abdulaziz has been outspoken on an ongoing diplomatic feud over human rights issues between Canada and Saudi Arabia. The targeting occurred while Abdulaziz, who received asylum in Canada, was attending university in Quebec. He has been a target of great interest to the Saudi government for several years. The Saudi government has tried to discourage his advocacy by revoking his scholarship to study in Canada in 2013, and threatening his family and friends in 2018.
- In Citizen Lab's September 2018 report, Hide and Seek: Tracking NSO Group's Pegasus Spyware to 45 Countries, they located a suspected infection in Quebec, Canada operated by what they inferred was a Saudi Arabia-linked Pegasus operator. Researchers matched the

pattern of infection to Abdulaziz's movements and found a text message with an infected link that looked like a notification from a mail package tracker.

- Citizen Lab was not aware of any legal authorization for the infection and monitoring of Abdulaziz in Canada by a foreign government. This means that the operators may have committed *Criminal Code* offences because these actions were not properly authorized under Canadian law.

Other Reports

Champing At the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware

Bill Marczak, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert

Marczak, Bill, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert. *Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware*. Citizen Lab, University of Toronto, December 6, 2017.
https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/.

Crux

This report explains how Ethiopian dissidents in the United States, United Kingdom, and other countries were targeted with emails containing sophisticated commercial spyware posing as Adobe Flash updates and PDF plugins. The targets included a US-based Ethiopian diaspora media outlet, the Oromia Media Network in Ethiopia, a PhD student, and a lawyer. One of the Citizen Lab report authors was also targeted. The analysis of the spyware indicates that it is a product called PC Surveillance System (PSS), a commercial spyware product with a novel exploit-free architecture manufactured and sold by Cyberbit, a cybersecurity company that is a wholly owned subsidiary of Elbit Systems.

Highlights

- This report describes a campaign of targeted malware attacks apparently carried out by Ethiopia. Targets received an email with a link to a malicious website impersonating an online video portal. Clicking on the link led to an invitation to download an Adobe Flash update containing spyware before viewing the video. In other cases, targets were prompted to install a fictitious app called “Adobe PdfWriter” in order to view a PDF file. The spyware appeared to be Cyberbit’s PSS product.
- Researchers identified a public logfile on the PSS spyware’s command and control server and monitored it over more than a year. Researchers saw the spyware operators connecting from Ethiopia and infected computers connecting from IP addresses in 20 countries, including IP addresses traced to Eritrean companies and government agencies.
- Internet scanning led to the discovery of other servers associated with PSS and several that appeared to be operated by Cyberbit. The public logfiles on these servers appeared to have tracked Cyberbit employees as they carried infected laptops around the world, apparently giving demonstrations of the PSS product to government authorities in Thailand, Uzbekistan, Zambia, the Philippines, and at ISS World Europe (Intelligence Support Systems for Electronic Surveillance) in 2017. Other demonstrations appeared to have been provided to France, Vietnam, Kazakhstan, Rwanda, Serbia, and Nigeria.
- The report contributes to a growing body of research showing the wide abuse of nation-state spyware by authoritarian leaders to covertly surveil and invisibly sabotage entities they deem

to be political threats. After FinFisher, Hacking Team, and NSO Group, Cyberbit is the fourth vendor of nation-state spyware whose tools Citizen Lab has seen abused. Ethiopia has also previously used Hacking Team's RCS spyware to target US-based journalists, as well as FinFisher's FinSpy spyware to target against political dissidents.

Tracking GhostNet: Investigating a Cyber Espionage Network

Information Warfare Monitor

Information Warfare Monitor. *Tracking GhostNet: Investigating a Cyber Espionage Network*. Information Warfare Monitor, March 29, 2009. http://www.nartv.org/mirror/ghostnet.pdf.

Crux

This report by the Information Warfare Monitor (Citizen Lab and SecDev) examines allegations of Chinese cyber espionage against the Tibetan community between June 2008 and March 2009. Field-based investigations were conducted in India, Europe, and North America. The fieldwork generated extensive data that allowed the researchers to examine Tibetan information security practices, as well as capture real-time evidence of malware that had penetrated Tibetan computer systems. The investigation uncovered a network of over 1,295 infected hosts in 103 countries. Up to 30% of the infected hosts are considered high-value targets and include computers located at ministries of foreign affairs, embassies, international organizations, news media, and NGOs.

Highlights

- Tibetan computer systems were conclusively compromised by multiple infections that gave attackers unprecedented access to potentially sensitive information.
- The GhostNet system directs infected computers to download a Trojan known as gh0st RAT that allows attackers to gain complete, real-time control. These instances of gh0st RAT are consistently controlled from commercial Internet access accounts located on the island of Hainan, People's Republic of China.
- GhostNet is capable of taking full control of infected computers, including searching and downloading specific files, and covertly operating attached devices, including microphones and web cameras.
- GhostNet uses social engineering to target its victims. Contextually relevant emails are sent to specific targets with attached documents that are packed with exploit code and Trojan horse programmes designed to take advantage of vulnerabilities in software installed on the target's computer.
- The report notes how there is a lack of awareness of cyber vulnerabilities and basic information security practices outside of the classified realm. Commercial computer systems, which represent most of the world's installed base, are insecure.

Shadows in the Cloud: Investigating Cyber Espionage 2.0

Information Warfare Monitor and Shadowserver Foundation

Information Warfare Monitor and Shadowserver Foundation. S*hadows in the Cloud: Investigating Cyber Espionage 2.0*. Information Warfare Monitor and Shadowserver Foundation, April 6, 2010. https://citizenlab.ca/wp-content/uploads/2017/05/shadows-in-the-cloud.pdf.

Crux

This report by the Information Warfare Monitor (Citizen Lab and SecDev) and the Shadowserver Foundation examines a complex cyber espionage network that compromised government, business, and academic computer systems in India, the Office of the Dalai Lama, the United Nations, and many other countries. Servers were found in Chengdu, China and are linked to the Chinese hacking community. However, the attackers' identities and the motivation for these attacks remain unknown. This report is a continuation of Information Warfare Monitor's Tracking GhostNet report that looked at allegations of Chinese cyber espionage against the Tibetan community. It also contributes to understanding the emerging attack vectors that started to leverage the vulnerabilities of network computing, peer-to-peer networks, and social networking in 2009-2010.

Highlights

- Data that was exfiltrated from politically sensitive targets included an encrypted diplomatic correspondence, as well as secret, restricted, and confidential documents. The *Shadow* network also exfiltrated over 1,500 letters sent from the Dalai Lama's office between January-November 2009.
- The report also documents how a tiered C&C infrastructure made use of freely available social media systems which directed compromised computers first to accounts on free web hosting services, and when the free hosting servers were disbaled, then to C&C servers in the PRC.
- Some of the findings of the report include how there is an asymmetry between the investments that governments, organizations, and other actors around the world make around adopting computerized administration systems and security policies and practices.
- Data leakage from malware networks can compromise unwitting third parties who are not initially targeted by the attackers. Data linkage from exfiltrated data can provide actionable and operational intelligence that can be used against a victim.
- Researchers note how we might be seeing the start of criminal networks being repurposed for political espionage as part of an evolution in signals intelligence. There is a blurring of the lines in malware genotypes among crimeware and more politically-motivated attacks which may be motivated to obscure attribution or part of a newly emerging market for commercial espionage products.

Exodus: New Android Spyware Made in Italy

Security Without Borders

Security Without Borders. *Exodus: New Android Spyware Made in Italy.* Security Without Borders, March 29, 2019. https://securitywithoutborders.org/blog/2019/03/29/exodus.html.

Crux

This report by Security without Borders examines a new Android spyware platform that they call named "Exodus." They believe that eSurv, an Italian company whose work is primarily in CCTV surveillance, developed the platform. eSurv has been developing intrusion software since at least 2016. Spyware was found on the Google Play Store disguised as service applications from mobile operators. Landing pages and decoys are all in Italian, with all victims located in Italy. Most of these apps collected a few dozen installations, with one app having over 350 installations.

Highlights

- Exodus is equipped with extensive collection and interception capabilities. When installed, the agent would open many vulnerabilities; sharing a wifi network with an infected phone could infect other phones. Data gathered from the intrusion was uploaded to Amazon Cloud.
- There was a lot of news coverage and interest by the Italian Prosecutor's office because the software was available for use by all law enforcement in Italy. About half of the public prosecutor's offices were using Exodus software, and all of the data from all offices was uploaded to a single Amazon Cloud service. eSurv also retained the data and accessed it on multiple occasions.
- Italian law requires that such law enforcement data must be physically stored in Italy and within the Prosecutor's network, meaning that the data was illegally sent to Amazon Cloud.
    - These regulations came after the highly publicized Hacking Team scandal where multiple investigative reports and leaked documents revealed how the Italian-based company was used to illegally spy on citizens by the Italian police. Hacking Team also sold commercial spyware products to governments with poor human rights records

Additional Resources

Security without Borders. Reports on Targeted Surveillance of Civil Society. https://securitywithoutborders.org/resources/targeted-surveillance-reports.html.

Siena Anstis. Litigation and Other Formal Complaints Concerning Targeted Digital Surveillance and the Digital Surveillance Industry. *Citizen Lab.* https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/.

Transparency Toolkit. Surveillance Industry Index. *Privacy International.* https://sii.transparencytoolkit.org/.

Glossary

Advanced persistent threat (APT): A term used to describe digital attacks that compromise computer systems with the intent of collecting data and monitoring communications without being noticed. They typically intend to persist for months or even years, and are generally associated with harvesting of information for political or economic purposes. The term is not to be confused with 'APT1,' the name given to a specific threat actor group (Citizen Lab, Communities @ Risk Glossary).

Attack vector: "A path or means by which a hacker… can gain access to a computer or network server in order to deliver a malicious payload."Methods include email, webpages, and instant messages (TechTarget). *See zero-click vector, and one-click vector.*

Backdoor: A method by which an attacker maintains access and control of a system after an initial compromise. This could be in the form of a hidden server listening on a port for an attacker to connect (Citizen Lab, Communities @ Risk Glossary).

Command and control servers (C&C or C2): Command-and-control (C2 or C&C) servers are computers used to send and receive commands and data to computers infected with malware. Upon being infected with malware, a compromised computer will attempt to contact a C&C, which issues it commands, sends additional malware to install, and exfiltrates data. C&C infrastructure can take different forms, with the most common being a domain name either registered or compromised specifically to act as a C&C. It is often possible to link different malware attacks together through their use of common C&C infrastructure (Citizen Lab, Communities @ Risk Glossary).

Commercial spyware: Commercial "lawful intercept" products and services that provide actors with turnkey surveillance solutions. The high cost of these products and the claim by vendors that sales are restricted to government clients make this primarily a state-centric route. Spyware is a piece of software that gathers and sends information about the computer it is installed on without the owner's consent or knowledge. Spyware ranges from web browser tracking cookies to expertly designed malicious programs (Citizen Lab, Communities @ Risk).

Deep packet inspection (DPI): A feature set attached to middlebox, network management or firewalls that refers to inspecting traffic at a level deeper than a stateful firewall (i.e. ip-src, ip-dest, src-port, dest-port). This is a dual-use technology. For example, DPI techniques can be used to block services like WhatsApp voice calling while allowing unrestricted access to WhatsApp text messages. It is a dual-use technology (Citizen Lab, Planet Netsweeper).

Demarcation point: The physical point where a public network ends and the customer's private network begins (Techopedia).

Domain name service (DNS): An Internet service analogous to a phone book that translates human friendly and easy-to-remember domain names to IP addresses. For example, DNS translates domain.com into the IP address 65.254.244.180 (Citizen Lab, Communities @ Risk Glossary).

Dual-use technologies: Technology that may serve a legitimate and socially beneficial purpose, or a purpose that undermines human rights depending on how it is deployed. These include *deep packet inspection (DPI)* tools and *Internet filtering technologies*, as well as *malicious software* like *malware* and *zero-day exploits*. Many dual-use technology companies are not transparent about the full range of products and services they sell or their clients, and the sector as a whole is shrouded in secrecy (Deibert, Dual-Use Technology).

Fingerprints: A unique pattern that identifies a technology. For example these can be obtained by combining data collected from outside network vantage point (i.e., through remote scans and publicly available datasets) and inside a country (i.e., principally through tests that make use of the OONI probe system) to verify if a specific device is being used for censorship(Citizen Lab, Planet Netsweeper).

Internet filtering technologies: Software that inspects, manages, and/or blocks our communications. When used at the level of large, consumer-facing Internet Service Providers (ISPs), Internet filtering technologies can have significant human rights impacts. They are considered a dual use technology. In the hands of authoritarian regimes, such professional services can limit the ability of citizens to communicate freely and help impose opaque and unaccountable controls on the public sphere (Citizen Lab, Planet Netsweeper).

Internet protocol (IP) address: A unique address that identifies a device on the Internet or a local network. It allows a system to be recognized by other systems connected via the Internet protocol. There are two primary types of IP address formats used today: IPv4 and IPv6 (Tech Terms).

Internet scanning tools: Software used to perform a complete scan of the entire Internet space in a matter of minutes. Think of this technique as an MRI of the Internet. It gives researchers the ability to identify equipment that is used to undertake Internet censorship and surveillance (Deibert, MRI of the Internet).

Internet service providers (ISPs): Consumer-facing companies that provide Internet connectivity services (Citizen Lab, Planet Netsweeper).

Malware (malicious software): Also known as malicious software, refers to software that is installed on a computer, often by deceit or trickery, that serves to disrupt operation, or gain unauthorized access to a given computer or its files (Citizen Lab, Communities @ Risk Glossary).

Middlebox: A specialty network device, appliance, or software that inspects network traffic and performs some action upon traffic that matches certain characteristics, such as throttling, dropping, or redirecting data traffic being sent to, or received from, sources that are being filtered or censored. A

middlebox is normally installed in between ISP subscribers and the outside Internet. It can use deep packet inspection techniques to classify traffic (Citizen Lab, Planet Netsweeper).

Network measurement methods: Methods that when employed provides insight into the quality, policies, or controls present in a computer network. For example, this includes using publicly available Internet scanning data from outside platforms like Shodan and Censys that probe most Internet-connected devices at regular intervals (Citizen Lab, Planet Netsweeper). It also includes existing Internet censorship data from sources like Open Observatory of Network Interference (OONI) and Information Controls Lab (ICLab) who collect data on Internet filtering and network interference from vantage points all around the world by convincing volunteers in various countries to run specialized measurement tools.

One-click vector: A malicious infection which only requires one click of a link to execute malicious code. For example, NSO Group's one-click vector involves sending the target a normal SMS text message with a link to a malicious website. The malicious website contains an exploit for the web browser on the target's device, and any other required exploits to implant the spyware (Citizen Lab, Million Dollar Dissident). *See attack vector, and zero-click vector.*

Remote access trojans (RATs): A software tool that allows a user to remotely access and control another computer. While remotely controlling a computer is a common and legitimate form of system administration, the term 'RAT' is used to refer to surreptitious and illegitimate access to a remote computer. While the sophistication of RATs can vary, they often have a similar set of capabilities, such as the ability to exfiltrate data, take screen captures, enable webcams/microphones, and install additional software (Citizen Lab, Communities @ Risk Glossary).

Signatures: How certain devices uniquely respond to the probes that Internet scans send. Certain filtering systems have the equivalent of digital signatures when probed. For example such signatures would allow researchers to locate middlebox installations around the world (Deibert, MRI of the Internet). *See fingerprints*.

Targeted digital threats: Persistent attempts to compromise and infiltrate the networked devices and infrastructure of specific individuals, groups, organizations, and communities. They are focused on specific targets, they persist over a period of time, and they are motivated by political objectives (Citizen Lab, Communities @ Risk).

Virtual private networks (VPNs): A method by which private computer networks can communicate through public networks. A commonly used VPN configuration, for example, allows remote employees to communicate with the computer network of their company. Malicious attackers sometimes use VPNs as a portion of their attack infrastructure (Citizen Lab, Communities @ Risk Glossary).

Virtual private servers: A virtualized computer server that is often sold by a company, for the purposes of hosting a website or publicly accessible Internet service. VPS servers can have their own copy of an operating system, providing the user with super-user privileges in the operating system and

enabling the user to install any kind of software on the OS (Techopedia; Citizen Lab, Communities @ Risk Glossary).

Voice-over-Internet-protocol (VoIP): Internet-based phone or voice communications service. Deep packet inspection tools can classify and block this kind of traffic.

WAP push: SMS protocol which is used as a transport for WAP – Wireless Application Protocol. WAP Push is a specially encoded message which includes a link to a WAP address. WAP is an old industry standard which was designed to deliver mobile web pages. WAP Push exploits can redirect a phone's web browser to a website with malicious code (Infosec Institute).

Zero-click vector: A malicious infection which does not require any action from a targeted individual. For example, NSO Group's zero-click vector uses a special type of SMS message like WAP Push Service Loading Service Load message which causes a phone to automatically open a link in a web browser, eliminating the need for a user to click on the link to become infected (Citizen Lab, Million Dollar Dissident). *See attack vector, and one-click vector.*

Zero-day (0-day) exploit: an attack that exploits a previously undocumented or unreleased flaw in software. Zero-day attacks are significant because they are difficult to discover (and hence costly for attackers to acquire and use) and difficult to defend against. They can be precious commodities, and are traded and sold by blackhat, greyhat, and legitimate market actors. Law enforcement and intelligence agencies purchase and use zero days or other malware—typically packaged as part of a suite of "solutions"—to surreptitiously get inside a target's device. When used without proper oversight, it can lead to significant human rights abuses (Deibert, Dual-Use Technology; Citizen Lab, Communities @ Risk Glossary).

Bibliography

Anstis, Siena, Ron Deibert, and Jon Penney. *Submission of the Citizen Lab to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on the Surveillance Industry and Human Rights.* Human Rights Council, June 2019. https://citizenlab.ca/wp-content/uploads/2019/02/Submission-to-the-UN-Special-Rapporteur-on-the-promotion-and-protection-of-the-right-to-freedom-of-opinion-and-expression-on-the-surveillance-industry-and-human-rights-2.pdf.

Anstis, Siena, Ronald J. Deibert and John Scott-Railton. *A Proposed Response to the Commercial Surveillance Emergency*. Lawfare, July 19, 2019. https://www.lawfareblog.com/proposed-response-commercial-surveillance-emergency.

Citizen Lab. *Communities @ Risk: Targeted Digital Threats Against Civil Society*. Citizen Lab, University of Toronto, November 11, 2014. https://targetedthreats.net/media/1-ExecutiveSummary.pdf.

Citizen Lab. *Reckless Reports: Abuse of NSO Group's Pegasus Spyware in Mexico (Series).* Citizen Lab, University of Toronto, 2017. https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/.

Dalek, Jakub, Ron Deibert, Bill Marczak, Sarah McKune, Helmi Noman, Irene Poetranto, and Adam Senft. *Tender Confirmed, Rights At Risk: Verifying Netsweeper in Bahrain*. Citizen Lab, University of Toronto, September 2016. https://citizenlab.ca/2016/09/tender-confirmed-rights-risk-verifying-netsweeper-bahrain/.

Dalek, Jakub, Lex Gill, Bill Marczak, Sarah McKune, Naser Noor, Joshua Oliver, Jon Penney, Adam Senft, and Ron Deibert. *Planet Netsweeper: Executive Summary.* Citizen Lab, University of Toronto, April 2018. https://citizenlab.ca/2018/04/planet-netsweeper/.

Deibert, Ron. What to do about "dual use" digital technologies? *Ronald Deibert [Blog],* November 29, 2016. https://deibert.citizenlab.ca/2016/11/dual-use/.

Fuchs, Christian. "Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society". *The Privacy & Security Research Paper Series, Issue #1*, 2012. http://fuchs.uti.at/wp-content/uploads/DPI.pdf.

GReAT and AMR. *New FinSpy iOS and Android implants revealed ITW.* Kaspersky, July 10, 2019. https://securelist.com/new-finspy-ios-and-android-implants-revealed-itw/91685/.

Hankey, Stephanie, and Daniel O Clunaigh. “Rethinking Risk and Security of Human Rights Defenders in the Digital Age.” *Journal of Human Rights Practice* 5, no. 3 (2013): 535-547. https://doi.org/10.1093/jhuman/hut023.

Information Warfare Monitor. *Tracking GhostNet: Investigating a Cyber Espionage Network*. Information Warfare Monitor, March 29, 2009. http://www.nartv.org/mirror/ghostnet.pdf.

Information Warfare Monitor and Shadowserver Foundation. *Shadows in the Cloud: Investigating Cyber Espionage 2.0*. Information Warfare Monitor and Shadowserver Foundation, April 6, 2010. https://citizenlab.ca/wp-content/uploads/2017/05/shadows-in-the-cloud.pdf.

Kaye, David. *Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.* Human Rights Council, June 2019. https://citizenlab.ca/wp-content/uploads/2019/06/Special-Rapporteur-report-Surveillance-and-human-rights.pdf.

Kazansky, Becky. *Digital Security in Context: Learning how human rights defenders adopt digital security practices*. Tactical Technology Collective, 2015. https://secresearch.tacticaltech.org/media/pages/pdfs/original/DigitalSecurityInContext.pdf

Le Blond, Stevens, Adina Uritesc, Cédric Gilbert, Zheng Leong Chua, Prateek Saxena, and Engin Kirda. “A Look at Targeted Attacks Through the Lense of an NGO.” *Proceedings of the 23rd USENIX Security Symposium*, August 20-22, 2014. https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/le-blond.

Marczak, Bill, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton. *Hacking Team and the Targeting of Ethiopian Journalists*. Citizen Lab, February 12, 2014. https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists/.

Marczak, Bill, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton. *Mapping Hacking Team’s Untraceable Spyware*, Citizen Lab, February 17, 2014. https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/.

Marczak, Bill, Claudio Guarnieri, Morgan Marquis-Boire, John Scott-Railton, and Sarah McKune. *Hacking Team’s US Nexus*. Citizen Lab, February 28, 2014. https://citizenlab.org/2014/02/hacking-teams-us-nexus/.

Marczak, Bill, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune. *Pay No Attention to the Server Behind the Proxy: Mapping FinFisher’s Continuing Proliferation.* Citizen Lab,

University of Toronto, October 15, 2015. https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/.

Marczak, Bill and John Scott-Railton. *The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against a UAE Human Rights Defender.* Citizen Lab, University of Toronto, August 24, 2016. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

Marczak, Bill, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert. *Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware*. Citizen Lab, University of Toronto, December 6, 2017. https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/.

Marczak, Bill, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, and Ron Deibert. *Bad Traffic: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?.* Citizen Lab, University of Toronto, March 2018. https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/.

Marczak, Bill, John Scott-Railton, and Ron Deibert. *NSO Group Infrastructure Linked to Targeting of Amnesty International and Saudi Dissident.* Citizen Lab, University of Toronto, July 31, 2018. https://citizenlab.ca/2018/07/nso-spyware-targeting-amnesty-international/.

Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*. Citizen Lab, University of Toronto, September 18, 2018. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

Marczak, Bill, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, and Ron Deibert. *The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil*. Citizen Lab, University of Toronto, October 1, 2018. https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/.

Marczak, William, and Vern Paxson. "Social Engineering Attacks on Government Opponents: Target Perspectives." *Proceedings on Privacy Enhancing Technologies, 2017*, no. 2 (2017): 172–185. https://doi.org/10.1515/popets-2017-0022.

Marquis-Boise, Morgan and Bill Marczak. *From Bahrain with Love: FinFisher's Spy Kit Exposed?*. Citizen Lab, University of Toronto, July 25, 2012. https://citizenlab.ca/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/.

Marquis-Boire, Morgan and Bill Marczak, and Claudio Guarnieri. *The SmartPhone Who Loved Me: FinFisher Goes Mobile?*. Citizen Lab, University of Toronto, August 29, 2012. https://citizenlab.ca/wp-content/uploads/2015/03/The-SmartPhone-Who-Loved-Me-FinFisher-Goes-Mobile.pdf.

Marquis-Boire, Morgan, Jakub Dalek, Sarah McKune, Matthew Carrieri, Masashi Crete-Nishihata, Ron Deibert, Saad Omar Khan, Helmi Noman, John Scott-Railton, and Greg Wiseman. *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools.* Citizen Lab, University of Toronto, January 15, 2013. https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/.

Marquis-Boire, Morgan, Bill Marczak, Claudio Guarnieri, and John Scott-Railton. *You Only Click Twice: FinFisher's Global Proliferation*. Citizen Lab, University of Toronto, March 13, 2013. https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

McKune, Sarah, Ron Deibert, Bill Marczak, Geoffrey Alexander, and John Scott-Railton. *Commercial Spyware: The Multibillion Dollar Industry Built on an Ethical and Legal Quagmire*. Citizen Lab, University of Toronto, December 6, 2017. https://citizenlab.ca/2017/12/legal-overview-ethiopian-dissidents-targeted-spyware/.

Mueller, Milton. *DPI Technology from the standpoint of Internet governance studies: An introduction.* Syracuse University School of Information Studies, October 21, 2011. https://pdfs.semanticscholar.org/17d8/e798bacba1d93f72d09c03f53857cd62222e.pdf.

Parsons, Christopher. "The Politics of Deep Packet Inspection: What Drives Surveillance by Internet Service Providers?." PhD diss., University of Victoria, 2013. Dspace Uvic https://dspace.library.uvic.ca/bitstream/handle/1828/5024/Parsons_Christopher_PhD_2013.pdf?sequence=6&isAllowed=y.

Penney, Jon, Sarah McKune, Lex Gill, and Ronald J. Deibert. "Advancing Human Rights-by-Design in the Dual-Use Technology Industry." *Columbia Journal of International Affairs* 71, no. 2 (2018): 103-110. https://jia.sipa.columbia.edu/advancing-human-rights-design-dual-use-technology-industry.

Privacy International. *The Global Surveillance Industry*. July 2016. https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.

Security Without Borders. *Exodus: New Android Spyware Made in Italy.* Security Without Borders, March 29, 2019. https://securitywithoutborders.org/blog/2019/03/29/exodus.html.