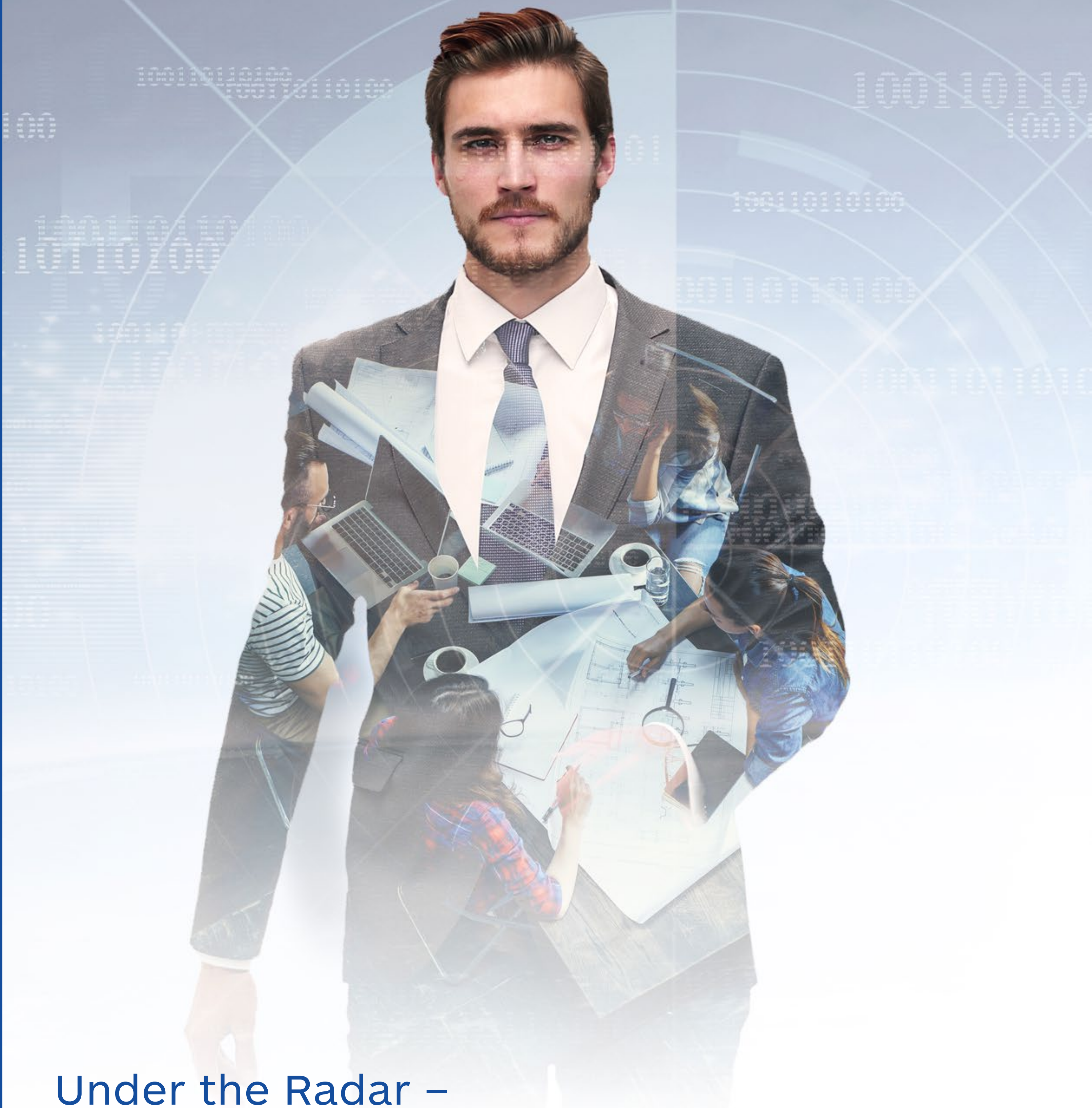

Under the Radar – The Future of Undetected Malware

Europe, Mideast, Africa

Adam Kujawa, Director of Malwarebytes Labs

Provided by

Malwarebytes LABS

The continuous evolution of cybercrime is a constant in our world. Almost everyday we're hearing about a new attack method, a new trick or tactic utilized by cybercriminals to infect users, steal their livelihood, and generally cause havoc.

To make money, today's cybercriminals want to completely own the targeted endpoint. They need to infect and avoid detection at both the moment they compromise an endpoint and during any attempts to detect them afterwards. It is logical to say that evasion of detection was once almost the singular, primary focus of malware authors. In fact, evasion and/or obfuscation-as-a-service became its own cottage industry: upload code, have it encrypted and verified as undetectable through scanning by all the major security detection engines, and then it is certified undetectable, sometimes with a money-back guarantee!

Recently, there was a noticeable shift in malware development methodology. Avoiding detection was one thing, but threat actors soon came to another realization: the longer they held the infected endpoint, the more their profit increased. As long as they survived attempts at remediation, they could turn the money taps back on.

For example, in the 2017 Cost of a Data Breach study by the Ponemon Institute and IBM, it was discovered that the mean time to identify an organizational breach was 197 days, while the time to contain that breach was 69 days. That is 266 days to remediate an attack. How much critical information do you think could be siphoned in 266 days? How much data was lost in the 69 days between the detection and containment? The time to remediate is far too slow given today's threats. In that time period, future malware will simply destroy or shake down your network for every penny.

Persistence—established by not only lengthening the time to detection, but also keeping a tentacle in the compromised device to later regrow the malware after detection—has now become as important to malware writers as avoiding detection. As a result, with this dual focus, a new class of malware has risen to prominence: under-the-radar malware. This difficult-to-remediate group of threats is growing in sophistication and frequency, a cause for concern for businesses today and in the future.

These sophisticated attacks avoid detection and maintain persistence by borrowing the propagation and anti-forensic techniques seen in the complex nation-state attacks of the past. Of these attacks, foremost in volume today are fileless attacks and compromises. These have had success in attacking businesses because the majority of past and present security solutions are designed to detect file-based malware. Those traditional security solutions, deployed at almost every business in the connected world, are simply not built to detect and remove malware that resides in memory rather than on the disk. This growing gap in protection has led to a tremendous increase in attacks, compromises, and resulting data theft from fileless attacks. in fact, fileless malware attacks are estimated to account for 35 percent of all attacks in 2018, and they're almost 10 times more likely to succeed than file-based attacks, according to a recent Ponemon Institute report.

> THREAT ACTORS SOON CAME TO ANOTHER REALIZATION: THE LONGER THEY HELD THE INFECTED ENDPOINT, THE MORE THEIR PROFIT INCREASED.

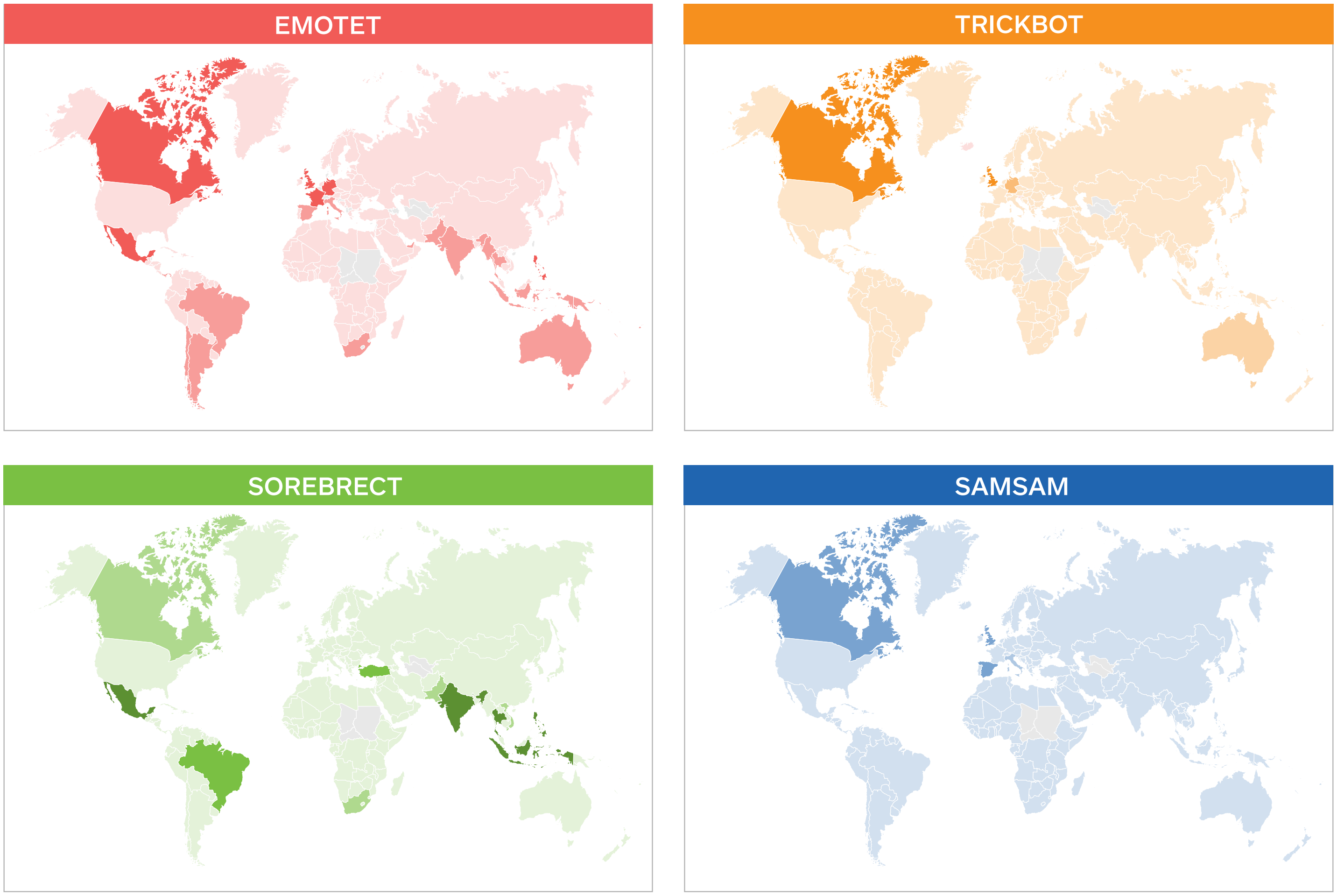

Figure 1. World-Wide Threat Map

Within our own detection and remediation telemetry, we have also documented a surge in these types of attacks. For example, in less than a month of observation, we recorded and prevented thousands of attacks in which a Microsoft Office document (Word, PowerPoint, Excel, etc.) attempted to launch malicious code likely to lead to a fileless attack. This number doesn't include attempts from exploit kits and other methods of infection.

Fileless malware is just one example among many attack methodologies currently evading traditional security defenses and maintaining persistence of compromise. Other forms of adapting attacks rely on specific actions designed to evade complete removal and remediation, when detected. From a single missed fragment of the exploiting code, the attacker can rebuild the infection and maintain the compromise.

This class of difficult-to-remove malware requires a new approach to stopping these threats before they create more damage to businesses.

The security industry is typically slow to respond to the latest threats, and is rarely able to stop new threats with old technology. Solutions are developed and deployed only after an attack type has already ravaged a business.

The security providers of today need to be able to pivot based on the newest threat vector and quickly develop the tools to combat it, because the future is not full of easy-to-detect junkware, but difficult-to-detect, difficult-to-remediate, sophisticated and dangerous malware. We've outlined a few of the latest threats to businesses, why they are dangerous, and what we can do to stop them.

Current Threats

Emotet and Trickbot

Finally, the banking trojan/downloader/botnet known as Emotet, along with its commonly seen accomplice TrickBot, are examples of the next generation of malware. These threats primarily use email distribution with malicious office documents using the same PowerShell attacks mentioned later to download and launch the malware.

The additional malicious files downloaded by the infection script are frequently mutated on the server side, to a degree by which you'll never see the same Emotet dropper twice. In addition, once on the system, these threats use the same vulnerabilities that WannaCry and NotPetya exploited (ETERNAL exploits and brute-forcing credentials) to traverse the network and spread their infection.

Certain industries were hit harder by these types of malware. As an example, Malwarebytes telemetry indicates the detection and removal of TrickBot malware nearly half a million times in the first nine months of 2018 within the education vertical (from primary schools to universities).

Emotet has been terrorizing systems worldwide for much of the year, with heavy campaigns in both Q1 and Q3 of 2018. In July 2018, US-CERT released an alert about Emotet and its capabilities.

Between January and September 2018, Emotet malware was detected and removed more than 1.5 million times using Malwarebytes. Emotet is most active in the United States, however there has been an increase in activity from both large and small countries, including the United Kingdom, Philippines, and Canada. In the UK and Germany, Malwarebytes detected more than 100,000 occurrences of Emotet in the first nine months of 2018 and nearly 60,000 instances of Emotet compromise have been detected by Malwarebytes in the Philippines.

In October 2018, Emotet was used to spread the Ryuk ransomware throughout the network of the Onslow Water and Sewer Authority in North Carolina.

Emotet & TrickBot in EMEA

Both of these families have notoriously been focused on western targets, while we see plenty of detections on the APAC side of these threats, its not until you get to the West (especially English-speaking countries) that you start to see true domination.

For Emotet then, it should be no surprise that the UK is the country with the most Emotet infections in Europe, at least in the last year.

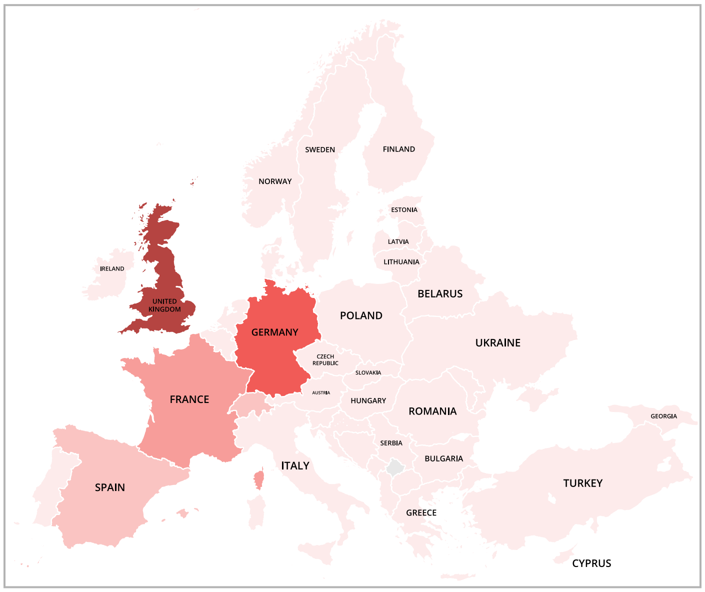

Figure 2. Emotet infections in Europe

Following the UK, Germany is the next top Emotet-infected country. This is actually very interesting because Germany has been known for a while as a country where new and interesting malware come from, we aren't entirely sure why. Germany isn't too kind to security researchers as many of the tools we use for analysis, penetration testing, etc., are outlawed in the country. These regional detection trends are very similar when looking at TrickBot detections.

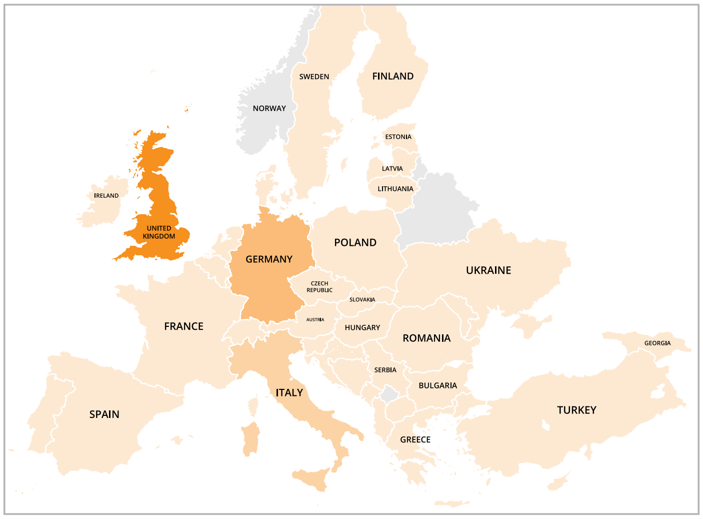

Figure 3. TrickBot infections in Europe

There are significantly more detections around Europe of Emotet then TrickBot, especially in France, Spain and Austria. However, if one assumes that TrickBot infections mainly come from Emotet infections, then you can expect that TrickBot is a result of Emotet not being detected and removed before it had a chance to drop more malware.

Considering how well Malwarebytes products deal with Emotet, one must assume that the infections of TrickBot in the UK and Germany are a result of after-the-fact scanning. Every organization that detected both Emotet and TrickBot should be concerned about their information having been stolen, including intellectual property, passwords, bank numbers, etc., because if the malware was able to get to the second stage dropping point, it may have had time to scrape the system for yummy data.

In February 2018, Allentown, PA's network was compromised by an Emotet attack, which resulted in the denied access of city employees, including law enforcement and financial specialists, to vital systems and processes that were disabled due to the infection. All in all, the city was looking at a bill of nearly $1 million to completely remediate the infection.

Emotet is a dynamic and multipurpose tool for cybercriminals. Copycats are going to take notice of this, and we will see Emotet clones throughout 2019. Specifically, authors will look to create malware that vertically infects an entire network, steals information, drops additional malware, and is churned out at breakneck speeds, mutating every dropper to avoid detection.

Will these specific families be able to last beyond the next shakeup within the threat landscape? Who knows. But the tech is solid and will remain. The tactics and techniques used by Emotet and TrickBot to remain undetected will continue well into in the future.

Sorebrect in EMEA

Sorebrect has most of its detections in APAC, however there are a few countries in EMEA that have detected the fileless ransomware, most notably Turkey. Greater detections in Turkey might be due to the reliance on older and more vulnerable technology, as is the case in APAC.

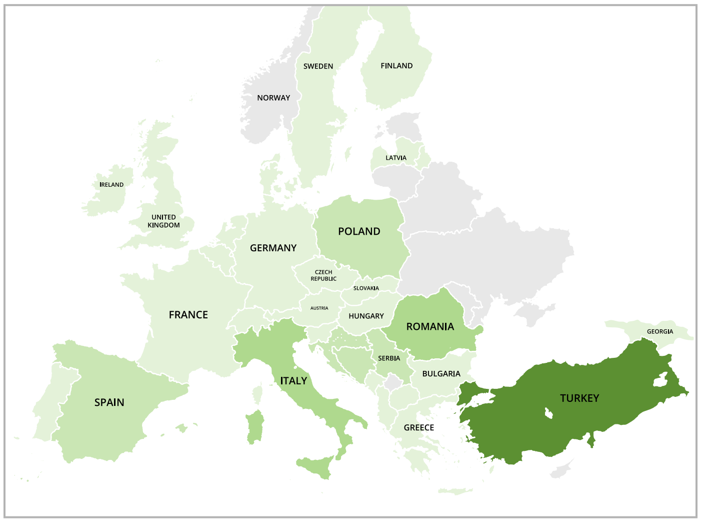

Figure 4. Sorebrect in Europe

Other noticeable activity in the APAC area involves exploit kits, or special code run in your browser that exploits an internet-facing application (browser) in order to install malware on the victim endpoint. For whatever reason, many countries in the APAC area are using older and less secure browsers and operating systems. Perhaps it's these same exploits that are being used to distribute Sorebrect, as fileless malware always works better when launched from a script.

Sorebrect is most known for infecting the networks of Middle Eastern countries in 2017, namely organizations working in the manufacturing industry.

When you combine that traditional ransom functionality with the fileless tactics of tomorrow, you've got a threat that is impossible to stop if you haven't a solution that watches process memory and uses behavioral identification. Lucky for us, this threat hasn't had a great spread and we haven't observed any copycats of this functionality making big splashes, either. However, it's just a matter of time before somebody perfects this infection method and using the computer becomes a lot scarier.

SamSam

Many of us tend to think of malware as completely autonomous. While many malware types, including bots, act similar to drones, there are malware types that are used primarily as tools for the attacker to manually launch whenever they need it, making the tool far more powerful than the drone.

One such tool is SamSam ransomware. After breaking into the network through known vulnerabilities or misconfigured services, SamSam is launched by attackers via an entirely manual process using batch scripts.

The reason this malware is difficult to remove is because before it is launched, attackers are able to manually disable security software. This is done after attackers gain administrative control of the system, mostly likely through an RDP exploit.

In a prominent example of SamSam compromise, the City of Atlanta has projected that they will spend $2.6 million on ransomware recovery.

According to one recent study, the attackers behind SamSam have struck 67 different targets in 2018, mostly in the US. We are likely to see SamSam, or a variant/copycat of it, continue to be an issue into 2019.

PowerShell

PowerShell is a trusted administrative scripting tool on Windows systems. While not itself malware, PowerShell can be abused to commit malicious acts. Attackers have been employing PowerShell as an avenue for compromise over the last couple of years.

Most often, we see PowerShell used in conjunction with a macro script in a malicious Office document.

In June 2018, a new method of using Office documents to attack users was released into the wild. The attack was able to exploit a vulnerability in the software and use PowerShell to download and install additional malware. This gives the attackers extraordinary capabilities, including launching fileless malware attacks directly into memory to evade detection by security vendors.

PowerShell was also used in a sophisticated attack against a Saudi Arabian government entity in 2017, along with VBScript and Office macro scripts. Further sign that the tools administrators use to make your system work, bad guys use to do the opposite.

Finally, the Emotet Banking Trojan malware and Dridex malware campaigns are great examples of the potential avenues for abuse afforded an attacker wielding PowerShell and employing macros in Office to compromise a victim.

Due to the success rate of this type of attack, the malware of the future is likely be fileless.

Current protection that's lacking

It's wishful thinking to believe that a single security product can provide complete protection from all threats in the wild, since the threat we face is not a single static attack. Instead, we face numerous highly dynamic attacks that are frequently modified to avoid detection by standard security products. If something works, a cybercriminal will repeat it. If it fails, they quickly adapt—and at much faster speeds than the capabilities of traditional tools.

Let's talk about what features traditional security solutions are lacking against today's threats. These are the deficiencies we are going to have to work through to be prepared for the future of cybercrime.

Traditional security solution shortcomings

There are three primary shortcomings with what we refer to as "traditional security" measures, including antivirus, that fail to utilize behavioral detection and a multi-layered approach to detecting and remediating threats.

Issue #1: Looking at only files

Malware takes a myriad of forms. When "traditional security" measures only look for traditional data and on-disk malware files, they see only half the picture that today's cybercriminal is painting. Modern security software goes beyond looking for files and process memory by also monitoring network traffic. This has been used as a beneficial indicator of compromise and a useful tool to identify attribution of hacker groups and malware developers.

Issue #2: Signatures

Probably the most commonly-referenced shortcoming of "traditional security" measures is that they rely heavily on human-created signatures. These are designed to help the product's detection engine identify threats from established rules created from observing the code of previous malware. This method of detection is still valuable in some situations.

However, if a solution is using signature-based detection as its primary or sole method of detection, then that product has already lost the cybercrime war. All the focus being given to this new method of malware development makes it hard for a signature-only approach to be prepared for the next iteration of threats.

Issue #3: Not checking process memory

One of the biggest differences between traditional security solutions and the "next generation" is the ability to monitor process memory. Every program that runs on a system has been allocated a certain amount of dynamic memory space, where it can store data necessary for its operation.

For years, modern malware has been using process memory to hijack legitimate processes for the sake of hiding network traffic or the malware itself. In some cases, malicious code is injected directly into a process from a script like PowerShell without a file. This is how fileless malware gets its name.

Current protection that's effective

As previously noted, the reliance on signatures alone is a mistake that many vendors are still currently making. However, the future of fighting cybercrime lies in being able to detect threats because they act like threats, not necessarily because you recognize them as such.

Behavioral detection

As mentioned, numerous times already, the reliance on signatures alone is a mistake that many vendors are currently making, however the future of fighting cybercrime lies in being able to detect threats because they act like threats, not necessarily because you recognize them as such. To that end, using behavioral detection that is dynamic and able to learn from the threats it encounters is going to be required to even stand a chance in the threat landscape of tomorrow.

Blocking at delivery

Having protection on each endpoint for what is running on that endpoint is very important for a good security posture, however an important aspect of fighting modern threats is identifying the danger before the threats can even tough the system, by focusing on the delivery mechanism.

Most malware is not spread by a shady guy in a fedora putting USB sticks into every computer he can see, it is spread through exploit kits and through malicious spam campaigns and often through avenues that can be monitored and protected. When you combine behavioral detection technology with monitoring entry points, you create a very powerful 'bouncer' for your systems that will keep your endpoints out of the 'potential victim' category.

Solution with self-defense modes

While not super common yet, the modern security solution needs to have a self-defense mode. This basically comes down to whether the security solution could deal with an attack that attempts to disable it or remove it from the system. More and more we see attacks that attempt to shut down security tools that may be used to detect and remove whatever additional payload the threat intends to infect the system with.

> ...THE FUTURE OF FIGHTING CYBERCRIME LIES IN BEING ABLE TO DETECT THREATS BECAUSE THEY ACT LIKE THREATS, NOT NECESSARILY BECAUSE YOU RECOGNIZE THEM AS SUCH.

Future of cybercrime

Finally, let's talk about what we are likely to see in the future of cybercrime. The families and tools we've covered so far are difficult to remove, detect and/or stop, however they are just the beginning of the next phase of malware development, where technologies like AI, worms and fileless malware are all going to be commonplace in the threat landscape. Here we talk about a few possible views of what the hard to remediate threats of tomorrow are going to be.

Artificial Intelligence used in the creation of malicious executables

While the idea of having artificial intelligence deployed (as in running on the victim system) WITH malware is pure science fiction, at least for the next 10 years, having malware created by and communicating with an AI is a very dangerous reality.

The criminals behind SamSam have only been able to launch a handful of attacks compared to families like Emotet, but with an artificial intelligence attacker, you can have the manual, dynamic benefits of a real person behind the keyboard, while also having the attack completely automated.

An AI that monitors what and how certain malware is detected can quickly make changes to evade detection for a new generation of malware. These defenses aren't just mucking up the code and hiding it within packed sections of a file, but rather new variants of the same malware appearing like legitimate files, with pseudo-authentic certificates maybe even built with the ability to disable security measures on the fly.

More 'Invisible' infections

Using tools like PowerShell, attackers have taken legitimate administration programs and turned them into a tool for fileless infection. The benefits to the cybercriminal in creating fileless malware are too great to ignore.

We should expect that some malware observed in 2020, maybe 2019, will use fileless infection techniques. They will likely be used in far more novel and dangerous ways than what we have seen so far.

The danger here is simple, more fileless malware equals more stealthy infections and more stealthy infections equals longer periods of time before the infection is found out, allowing the attackers to do the maximum amount of damage to a system or network, be it for spying, ransoming or some other nefarious purpose.

Businesses will become 'worm food'

In 2017, WannaCry made headlines by quickly infecting and spreading through networks all over the world, using exploits obtained from government leaks. To this day, there are still WannaCry detections from systems that were never patched and continue to get infected with WannaCry as it automatically spreads itself as far as it can.

Now we have seen this same technology used within information stealing malware like Emotet and Trickbot, making them difficult to completely remove if the infection is not contained in a timely manner. Expect the next generation of 'worms' to be faster, stealthier and likely come with a swiss army knife of nefarious functionality.

The best targets for these types of threats are groups of networked computers, which you most commonly find within businesses. Due to the higher ransom demand possible, the value of the information being stolen and the ease of spreading an infection with modern malware, tomorrows malware, at least the real dangerous stuff, is going to be very focused on infecting businesses and once an infection happens, unless there are solid security solutions deployed to stop it, the infection will spread at alarming rates.

Conclusion

Our adversaries will always look where we are not looking. That's just the nature of warfare—even cyberattacks. With state-sponsored, highly-sophisticated threats discussed on the nightly news, it's only a matter of time before these methods become commonplace.

For the best chance of protecting and remediating against these newer forms of malware, we need solutions of the future, for the future. Tools that can modify and refine detection and remediation capabilities, no matter what the criminals throw at us. We need every aspect of the computing experience to be monitored and secured, including incoming and outgoing traffic to which processes can run and even which files can be downloaded.

Right now, we develop shields. As with any armor, a crack on a shield can lead to its compromise. In the future, we need more than a shield; we need a smooth orb of protection with no cracks, and a dynamic and reflective skin giving the user a full view of what is out there, what is trying to get in, and what is hiding under the radar.

> WE NEED EVERY ASPECT OF THE COMPUTING EXPERIENCE TO BE MONITORED AND SECURED, INCLUDING INCOMING AND OUTGOING TRAFFIC TO WHICH PROCESSES CAN RUN AND EVEN WHICH FILES CAN BE DOWNLOADED.

blog.malwarebytes.com corporate-sales@malwarebytes.com ☎ 1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.