SafeBreach

HACKER'S PLAYBOOK

A Ransomware Special Edition

July 2017 | Analysis of findings by SafeBreach Labs

SafeBreach Labs

ABOUT THE HACKER'S PLAYBOOK

First published in Q1 2016, the SafeBreach Hacker's Playbook is the first to report enterprise security trends and risky behaviors from the point-of-view of an "attacker". How do we actually simulate a hacker?

We deploy simulators across endpoints, network and cloud; these simulators play the role of a "virtual hacker" and execute breach methods from our hacker's playbook. This allows us to quantify actual risks and validate whether security controls in the environment are working as expected. The insights from these deployments are incorporated in the Hacker's Playbook report.

We're excited to kick off a "Special Edition" that focuses on a specific type of attack that's in the headlines.

As always, our goal is to give you the perspective of the hacker – a point of view that we find is sorely missing in most security organizations. In order to properly understand your risks, validate your security controls and better prioritize your resources, you must play the role of an attacker. By putting yourselves in the mindset of an attacker, you can better anticipate how well security controls will work against actual attacks, allowing you to quickly take corrective action on the things that matter.

This Special Edition is focused on Ransomware for three reasons:

- **Top of mind concern:** Many security organizations we worked with were worried about ransomware. In fact, it is one of the highest volume "attack searches" on Google, with almost 170,000 searches a month. In April 2016, the FBI issued a warning about ransomware attacks on the rise [1]. In fact, according to the 2017 Verizon Data Breach Investigations Report[2], ransomware has moved from the 22nd most common variety of malware in the 2014 DBIR to the 5th.

- **Booming business:** Over the past five years, ransomware attacks have grown, along with the corresponding ransom. Estimates from the FBI indicated that ransomware is a $1B dollar source of income[3], with the average ransom per machine in the amount of $679 in 2016, more than double the $294 average ransom in 2015[4]. Symantec's recent report indicates that in 2017, this number has risen to $1077[5].

- **Multi-vector attack:** From the perspective of a "virtual hacker", we find ransomware targeted at enterprises to be an extremely interesting attack that challenges almost every single security product deployed—from email security, secure web gateways and next-generation firewalls, to intrusion prevention systems and endpoint security. Ransomware also strongly advocates for a defense-in-depth approach, and the need for controls across the entire cyber kill chain.

OVERVIEW

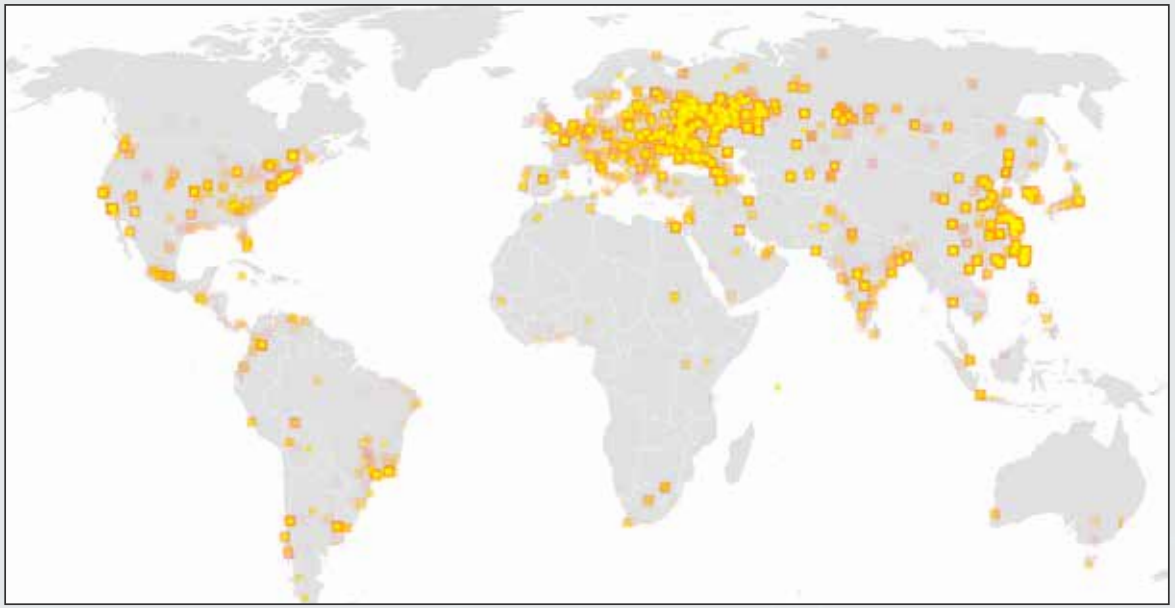
We started working on this document in early Q2 this year, as a "Special Edition" version of our annual Hacker's Playbook. About halfway through our research and analysis for this document, WannaCry hit the headlines.

According to the Federal Bureau of Investigation[7], on average 4000 ransomware attacks occur daily. In May 2017, WannaCry infected 230,000 computers across more than 150 countries in just 48 hours before it was stopped[8]. James Schlesinger's quote rang true for many security organizations, "We have only two modes—complacency and panic," as many scrambled to patch or deal with the aftermath of the attack.

In less than 24 hours, SafeBreach Labs delivered WannaCry breach methods (infiltration of the ransomware, download/save to disk and C2 communications) to our customers to validate that their security controls were working.

One major enterprise spent two days updating and patching 40,000 endpoints, and used SafeBreach to confirm the updates they had made were actually working. WannaCry is incorporated in this report, and (no surprise) is one of the most successful infiltration methods we used followed by older ransomware like CryptoLocker.

WannaCry Infection Map



Source: New York Times WannaCry infection map[9]

Here are some of our key findings from this report:

1

TOP SUCCESSFUL RANSOMWARE DOWNLOADED IS WANNACRY

The WannaCry analysis is included in this report, and as expected, is one of the top successful infiltration breach methods we used.

2

ENCRYPTED TRAFFIC IS A BLIND SPOT

We simulated a variety of infiltration methods, and found the most success with HTTPS traffic.
Most security organizations did not inspect encrypted traffic, leaving them blind to SafeBreach simulated attacks.

3

EMBEDDED EXECUTABLES BYPASSED SECURITY PRODUCTS

Most security products in our customers' deployments would block a traditional executable, but did not stop executables embedded within a variety of file formats.

4

MULTIPLE RANSOMWARE SUCCEEDED WITH C2 COMMUNICATIONS

The majority of security teams aren't inspecting outbound connections, enabling us to successfully simulate C2 communications without being detected or blocked.

5

OLD RANDSOMWARE STILL SUCCESSFUL

Other than the WannaCry, a fairly new attack, the majority of ransomware that we used (for example: CryptoLocker) were several years old; yet we were still successful. In some cases, the right security practices weren't in place; in other cases, it was a misconfigured security product.

THE WHAT AND WHY OF RANSOMWARE

Ransomware is a type of malware that prevents user access to their system or data by encrypting the data or files on the device. Decryption keys are provided once the ransom has been paid.

Ransomware has become a financially rewarding weapon for cyber attackers. Ransom prices depend on the data and the victim. As described earlier, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. This is a 300-percent increase over the approximately 1,000 attacks per day seen in 2015[10].

From a monetary angle, ransomware victims shelled out $24 million in all of 2015 but by 2016, in the first three months alone, victims had paid out $209 million. According to the FBI[3], $1B in ransomware payments were paid in 2016.

It's no surprise then why ransomware attacks have increased in the last three years – there is better reward/risk ratio, there is an untraceable payment method and there are multiple ways to infect very large numbers of victims.

Three reasons ransomware attacks have increased:

Untraceable payments

The lack of an untraceable payment method has been one of the biggest barriers with ransomware. With the emergence of Bitcoin, cybercriminals now have a hard-to-trace method for victims to pay them. Bitcoin wallets can be easily generated for each infection, making it easy for attackers but complicated for law enforcement to follow the money trail.

Better reward/risk ratio

The criminal Willie Sutton was once asked why he robbed banks, and his response was simple -- "Because that's where the money is". The recent 2017 Verizon Data Breach Report[1] states that ransomware is the reigning champion in Crimeware, and the number of attacks will increase each year. As a cyber criminal, ransomware is a great way to make a living because it represents low risks and high rewards. An attacker just needs to encrypt a user's data instead of moving laterally into the network and looking for sensitive data. Even though the FBI continues to advocate that organizations should not pay a ransom to recover their data, there are many high-profile organizations such as the Hollywood Presbyterian Medical Center[11] that have done so, and will continue to do so if attacked.

Widespread infection

There are myriad ways to infect very large sets of users very quickly via mass phishing campaigns. Additionally, ransomware as-a-service programs are available for novice cybercriminals where the author of the ransomware takes a cut of the profits while his/her affiliates focus on infection.

HACKING ACME CORP

A VIRTUAL HACKER PERSPECTIVE

If you've read our Q4 Hacker's Playbook report[12], you know that we've been successful at breaching environments protected by some of the most comprehensive security controls. We were successful using old exploit kits and executables to infiltrate the network, we took advantage of misconfigured malware sandboxing products,and bypassed security segments. We also continue to hold a 100% success rate in data exfiltration in all of our deployments.

Knowing all this, how would we design a ransomware attack?

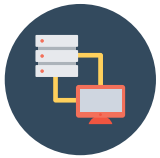
We would use many of the successes outlined above. Ransomware infiltrates and propagates in the same ways as any other malware. The primary difference is that the last step for ransomware is encryption rather than data exfiltration. You can see that each of these different phases challenges different security products.

Infiltration

There are multiple ways ransomware can infect an organization. Certain techniques such as malicious emails and exploit kits tend to be more successful compared to others. In our case, we would take advantage of social engineering to get Bob at Acme Corp to click on a link and download a file containing ransomware. Alternately we could use the techniques involved in WannaCry, wherein we would instead cleverly package our dropper into an otherwise innocuous file, like an AOL IM installer, or a malicious PDF.

Ransomware written to disk

Bob at AcmeCorp saves the attachment on his computer. An endpoint security or malware sandboxing product should have detected that the attachment contained an executable file and warned Bob, and prevented this action from taking place. If the attachment seemed innocuous, but an executable called out for further payloads, network scanning tools should see that malicious traffic, either outbound or inbound, and block the communication and subsequent payload.



Ransomware talks to command and control

In some cases, before the ransomware can start attacking, it will contact the command and control server operated by the attacker. The ransomware client and server identify each other, and share cryptographic keys. This allows the attacker to store one key on Bob's computer, and the other key on their server for decryption once the ransom is paid. This C2 communication should be inspected by a firewall looking at outbound connections. Most of the time, this may not stop the ransomware attack, but it would at least initiate the beginning of an investigation and prevent further infections As an attacker, our communication would be via SSL as the majority of organizations don't decrypt and inspect SSL traffic. In certain ransomware cases, this C2 communication does not occur. For example, Cerber is a ransomware which can encrypt files in offline mode, it doesn't need to fetch the keys from the C2 server.

Ransomware executes and encrypts files

The final step for the ransomware is searching for files on Bob's computer, and encrypting them. Once the files are encrypted, the victims are shown a lock screen demanding ransom.

RANSOMWARE INSIGHTS FROM SAFEBREACH DEPLOYMENTS

Now that we've outlined the steps we'd take for the "perfect ransomware crime," how does this idealized version compare with what actually works in actual SafeBreach customer environments? Specifically, we wanted to gain more insights on our successes as a virtual hacker and which methods were most effective. We wanted to be able to answer the following:

- The top techniques to get ransomware on an organization's computer?
- Top ransomware that was successful infiltrating an organization?
- How we were able to install ransomware on disks?
- What were the top ransomware we were able to install on disks?
- What were the top ransomware we used that performed C2 communications?

INFILTRATION FINDINGS:

Encrypted Traffic A Blind Spot

We simulated a variety of infiltration methods, and found the most success with HTTPS traffic. When it comes to success rate overall: HTTPS wins over HTTP, 443 wins over 80 and 8080. This isn't a surprise. A significant amount of traffic is already encrypted on corporate networks, and because most security organizations don't decrypt traffic, it is easy for an attacker to slip past any security solution undetected. Encrypted traffic is a blind spot for most security teams.

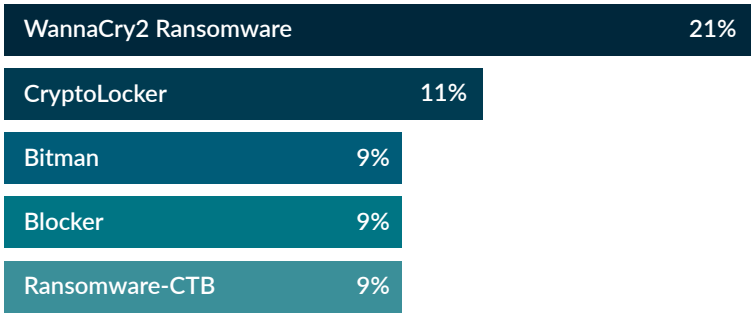
Top Infiltration Techniques Via Executable Files

With ransomware simulations, the top infiltration techniques were via executable files delivered over HTTP/S. We drilled a little deeper into the data to see which three methods were most successful; here are the top 5:

- EXE inside a VBS - Visual Basic is a scripting language that MSFT supports. SafeBreach was successful in breaching an environment using both an executable file hidden in VBScript, and by packing the executable within the scripts we were able to bypass deep packet inspection.
- EXE inside a DOC with macro - Microsoft Office™ for many years contained macros that allow you to program custom events. Over the years, attackers have abused macros to create malware. In fact, in June 2016, the US Cert issued a warning about the resurgence of using macros but it appears most organizations are still struggling with the balance between business continuity and security.
- EXE inside encrypted zip - In this example, SafeBreach used encrypted ZIP file/archive over HTTP. One of the oldest tricks by attackers, encrypted zip files over HTTP should be limited by policy or inspected by next-generation firewalls.
- EXE inside JAR - "JAR" is a package file that aggregates many Java class files and associated metadata and resources (text, images, etc). In this example, SafeBreach embedded an executable file within JAR for exploitation and malware delivery.
- EXE dropper inside a PPT with macro - A dropper is a program that has been designed to "install" some sort of malware (virus, backdoor, etc.) to a target system. In this case, we embedded the dropper within a powerpoint with macro.

WannaCry Tops Successful Ransomware Installed

The top 5 ransomware malware samples we used, based on success quantity were:

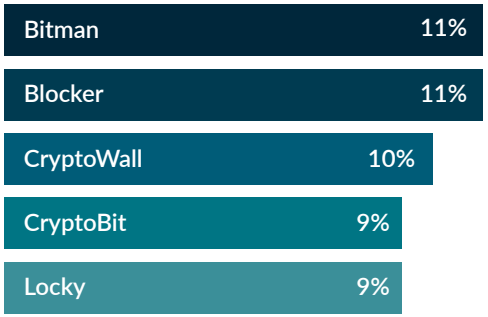


WannaCry2 clearly needs no introduction, and was one of the more successful ransomware utilized by SafeBreach. Others included CryptoLocker, ransomware from 2013 and 2014 targeting Microsoft Windows; Bitman or TeslaCrypt, a ransomware from 2015 targeting gaming files. Blocker and Ransomware-CTB round up the top 5.

RANSOMWARE WRITTEN TO DISK:

Top Five Successful Ransomware Dropped To Disk

Bitman, Blocker and Cryptowall topped the list of successful ransomware we were able to write to disk in our simulations.

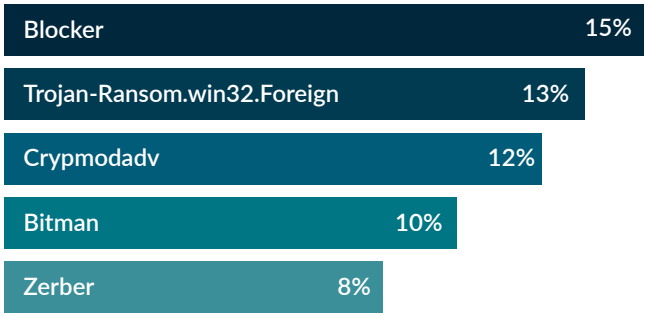


When we simulated ransomware written to the disk, typically the second phase of a ransomware attack, many different types of ransomware were successful. Similar to the results from successful ransomware installed, the biggest surprise to us was the success of ransomware that had been around for many years. In these customer deployments, endpoint security products that should have stopped SafeBreach from dropping ransomware to disk did not do so. In some cases, we found products that were misconfigured or simply didn't work.

RANSOMWARE C2 COMMUNICATIONS:

Blocker Tops Successful Ransomware Executing C2 Communications

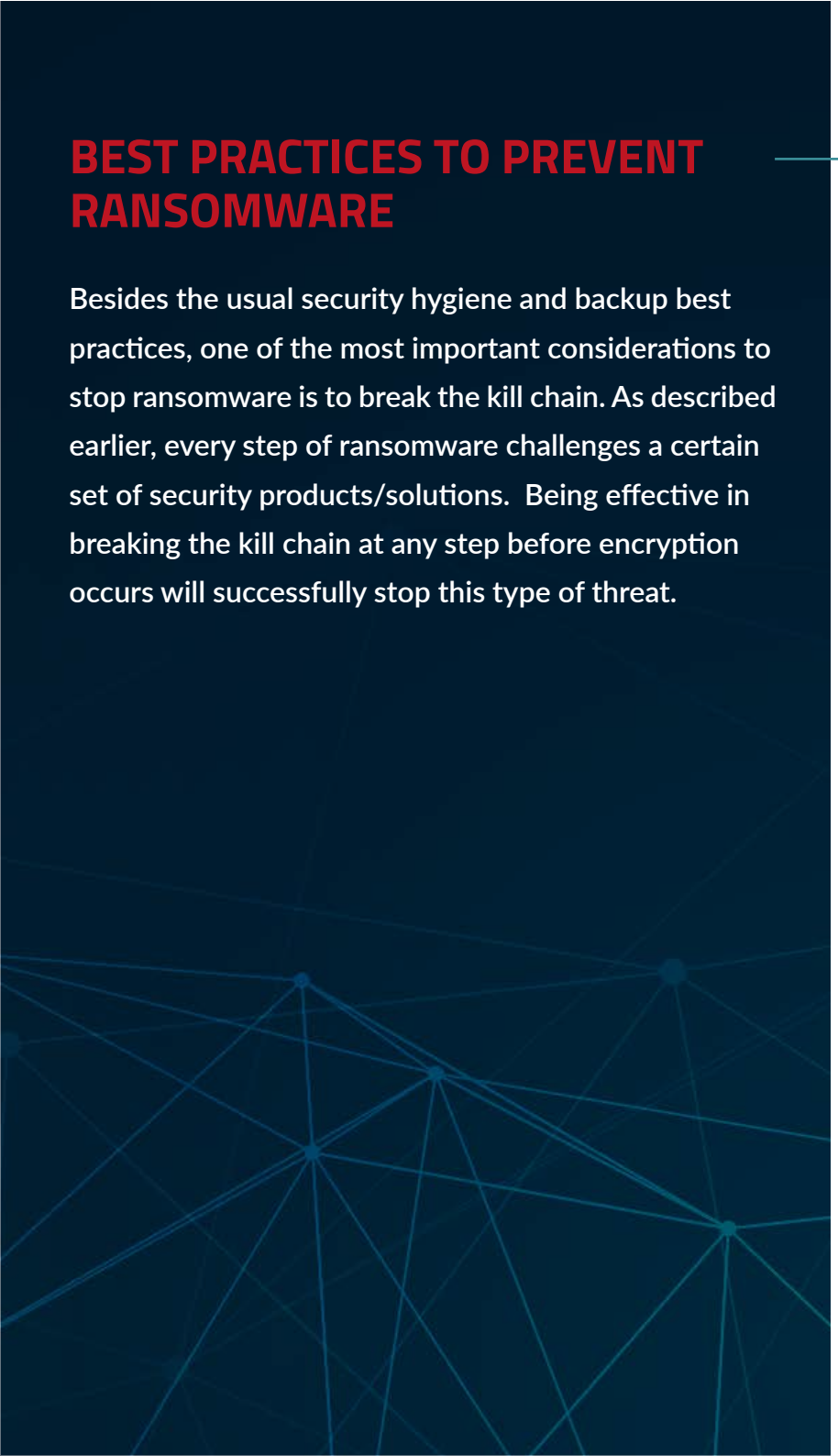
We simulated C2 communications from various ransomware, and the following were the top five:



C2 communications does not always occur with all ransomware, but when it does, it's an opportunity to detect an attack in progress and stop more endpoints from being infected. SafeBreach simulated C2 communications to challenge security products that should have inspected this traffic. The top 3 in success quantity were Blocker, Foreign and Crypmodadv.

BEST PRACTICES TO PREVENT RANSOMWARE

Besides the usual security hygiene and backup best practices, one of the most important considerations to stop ransomware is to break the kill chain. As described earlier, every step of ransomware challenges a certain set of security products/solutions. Being effective in breaking the kill chain at any step before encryption occurs will successfully stop this type of threat.



Eliminate Blind Spots

Ransomware payloads aren't any different from other types of malware. Security teams need to control what's coming into the organization and eliminate their blind spots. This means:

- Blocking exploit kits that point users to either visit a site that contains malicious exploit code, or to download a seemingly legitimate file with hidden malicious code
- Inspecting encrypted traffic (HTTPS/SSL) that hides user actions
- Blocking macros or hidden executable file formats that may not be inspected by email security or endpoint security malware sandboxing solutions

Control What's Being Saved

With the right endpoint security solution, you can blacklist known signatures or hash of files for ransomware, or prevent potentially malicious files being saved to the disk. Ensure that endpoint security solutions deployed are scanning all folders including temporary folders.

Inspect C2 Communications

Some ransomware families need to call home to establish the encryption keys. Inspect the command and control communications using a next-generation firewall, proxy, or IPS. Blocking the C2 communications may not stop a ransomware, but you'll be able to alert and begin investigation to prevent more computers from being infected.

Don't Wait - Simulate!

Utilizing breach and attack simulation technology allows security teams to validate whether the security controls they have deployed to stop ransomware are working. Breach and attack simulations allow you to also visualize the entire kill chain so you can observe where to focus security efforts. Most importantly it validates all security controls before attackers do the testing instead.

Back Up That Data

Backups are critical in ransomware incidents; if you are infected, backups are often the best way to recover your critical data. It is important to not only regularly back up data but also verify the integrity of those backups to ensure the right data is maintained, and that malicious payloads are not accidentally propagated. Periodically running a data restoration drill would also be a good idea.

SafeBreach

FOOTNOTES

[1]https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise
[2] Verizon Data Breach Investigation Report, 2017
[3]http://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646
[4]http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf
[5]https://www.symantec.com/security-center/threat-report
[6]Trend Micro 2016 Security Roundup https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup
[7]https://www.justice.gov/criminal-ccips/file/872771/download
[8]http://www.telegraph.co.uk/news/2017/05/12/nhs-hit-major-cyber-attack-hackers-demanding-ransom/
[9]https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html
[10]https://www.fedscoop.com/ransomware-attacks-up-300-percent-in-first-quarter-of-2016/
[11]http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html
[12]https://go.safebreach.com/Website-Content-Report-Hackers-Playbook-Second-Edition-LP.html

SafeBreach 111 W Evelyn Avenue Suite 117 | Sunnyvale, CA 94086 | contact@safebreach.com