Exhibit H

2018 SONICWALL CYBER THREAT REPORT

Threat Intelligence, Industry Analysis and Cybersecurity Guidance for the Global Cyber Arms Race

Exhibit #

McDuff-4

11/02/2020

exhibitsticker.com

sonicwall.com | @sonicwall

SONICWALL®

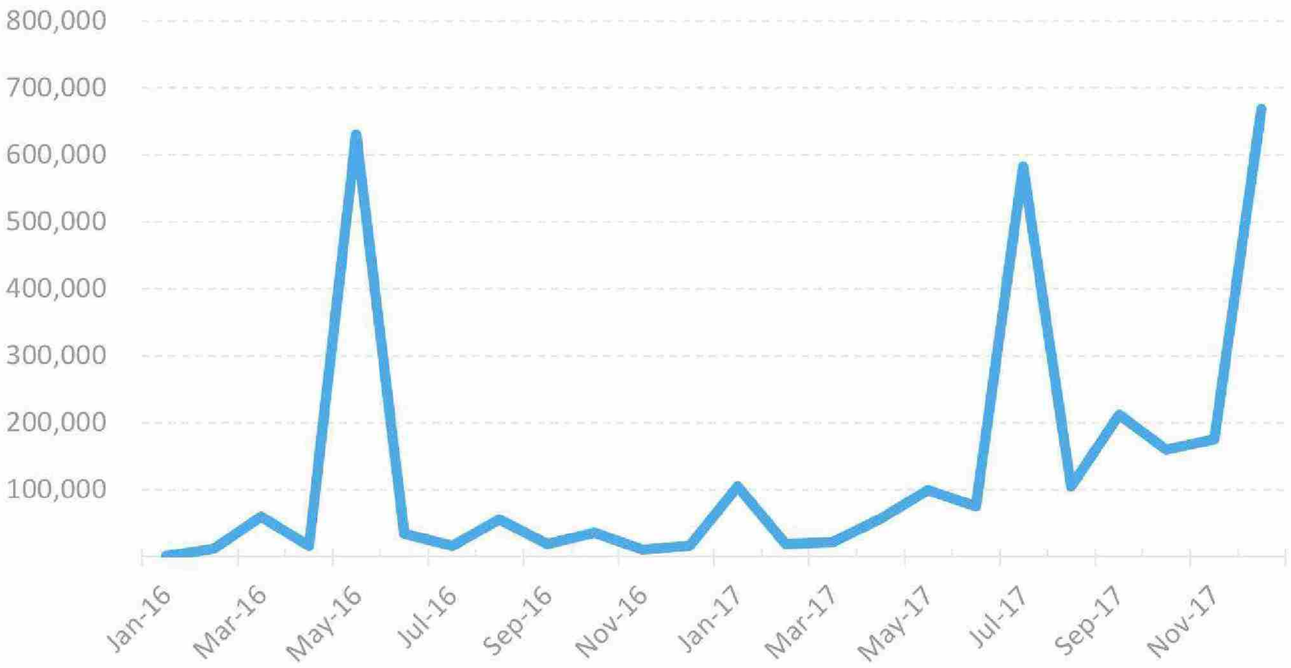
As outlined, the use of encryption to protect web traffic was up 24 percent in 2017. With this growth, each year provides cybercriminals more and more avenues for obscuring their malicious actions. For example, the use of SSL to download Nemucod content increased in 2017.

Leveraging intrusion prevention systems (IPS), SonicWall recorded and analyzed similar trends for attempted network intrusions. The top IPS attacks focus on HTTP Header, Directory Traversal and SQL Injection.

Encrypted traffic will continue to grow, but unencrypted traffic will remain for most public services. However, threat actors will continue to use encryption to hide attacks in 2018 and beyond.

In response, more organizations and enterprises are implementing SSL decryption, inspection and mitigation capabilities into their security strategy.

Malware Attacks Over SSL by Month



MALWARE COCKTAILS STILL MIXING THINGS UP

The data presented to this point highlights changes in cybercriminal behavior. Cybercriminals are mainly relying on existing code — with a few minor changes — to build malware variants that can spread quickly and more dangerously. All with the purpose of avoiding detection. This is the malware cocktail.

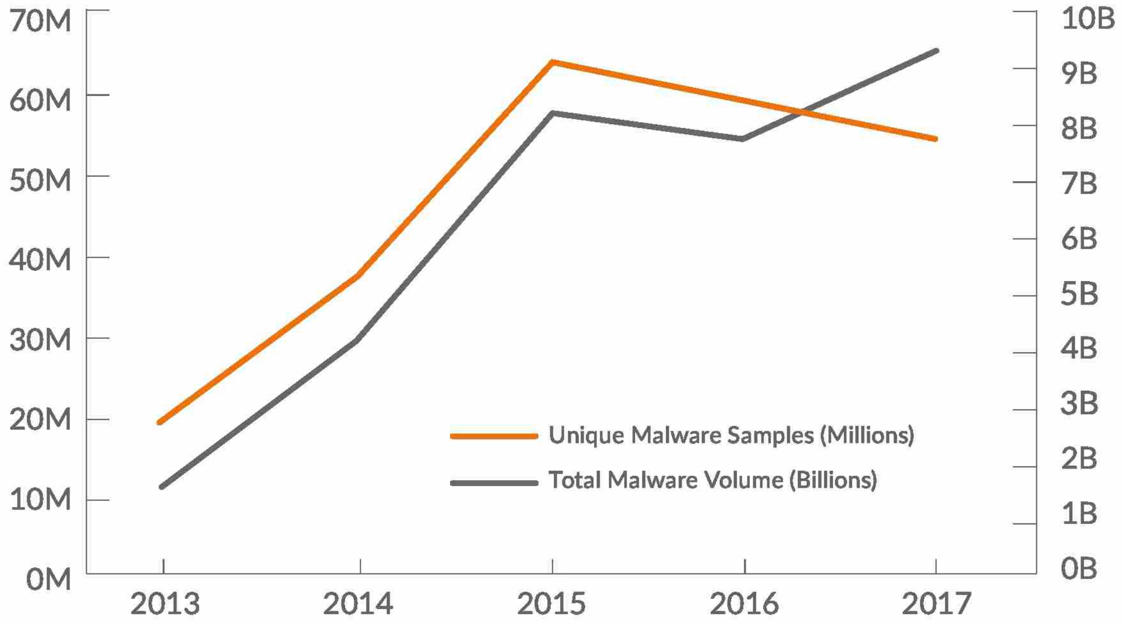
As an example, while the total volume of malware attacks was up, the number of unique malware signatures declined. In 2017, SonicWall collected **56 million unique malware samples** in contrast to the 60 million samples discovered in 2016.

For the year, unique malware signatures dipped 6.7 percent from 2016 and 12.5 percent from 2015. However, 2017 levels remain 51.4 percent higher than the 2014 mark.

SonicWall Capture Labs uses machine learning to examine individual artifacts of malware signatures to categorize each as unique or something that already exists. This helps reduce the number of new signatures needed to effectively mitigate known and unknown malware attacks.

The reason? Malicious groups are still using the same malware — with slight tweaks and modifications — as seen in years past. But threat actors aren't just re-tooling old malware code and launching it haphazardly. While some of that still occurs from 'script kiddies' and other less-skilled hackers, innovative authors are refining how they target their victims.

Rise of the Malware Cocktail



Evolving malware tactics

Take Cerber, for example. It's a Trojan that mainly spreads via email spam, but also leverages exploit kits (EK), such as Magnitude EK in September 2017. It also was one of the top attacks that used encryption to avoid detection.

What's noteworthy about Cerber is its ability to evolve in a short period of time. SonicWall Capture Labs threat researchers were identifying updated versions of Cerber being caught in the wild — as many as two versions a day.

These were **malware cocktails** created by cybercriminals to elude signature-based security solutions. Even more interesting, the new Cerber variants were utilizing seven different tactics to evade detection.[xxx]

Hits vs. Detection

Signature Detection
The number of attacks, by the malware type and its variants, caught by the signature.

Malware Hit
The recognition of a malware attack. Once detected, the attack is blocked.

New exploit kits, old code

SonicWall Capture Labs threat researchers aren't discovering many new exploit kits. What they are finding, however, are EKs that repurpose old code for new gains.

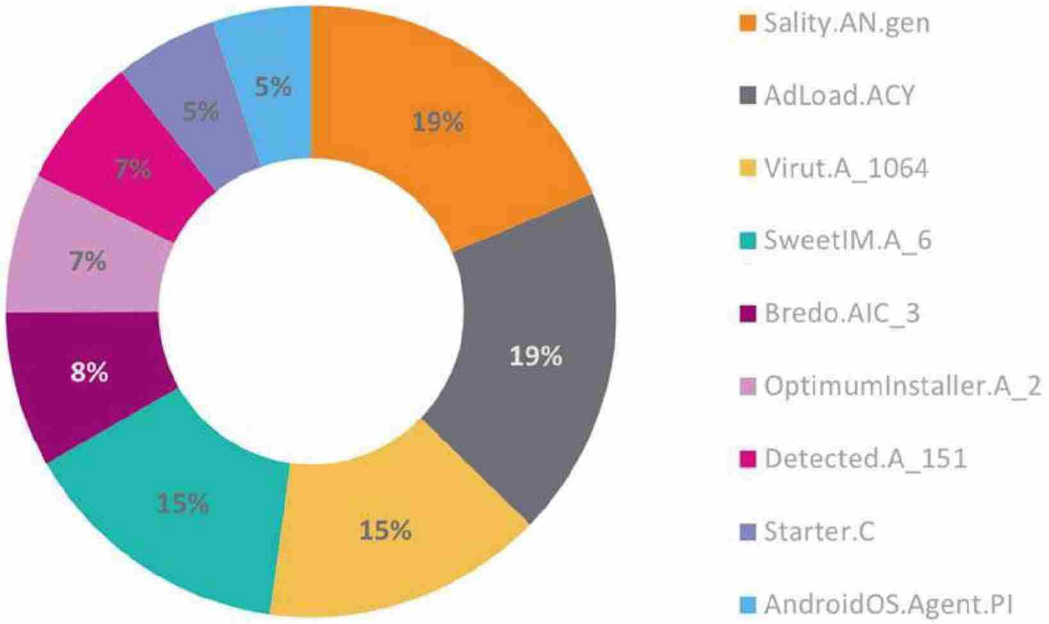
Terror, for example, was an exploit kit first noticed in early 2017. Then a new version of the Terror exploit kit appeared, which seemed to be based on code stolen from both the RIG and Sundown exploit kits.[xxxi]

The Terror landing page consisted of a JavaScript that appeared to be taken from RIG, followed by another script stolen from Sundown. This stolen JavaScript was followed by embedded Flash exploits. There is no obfuscation seen in this exploit kit, and both the landing page and payload are unencrypted.

Similarly, the exploit kit Nebula was discovered in February 2017. It was likely a variant of Sundown and spread the DiamondFox and Ramnit malware, among others.[xxxii]

Agile malware cocktails, coupled with new propagation methods (e.g., NSA exploits, remote desktop protocols, toast overlays), show that some cybercriminals are still at work mixing and matching malware attacks to circumvent defenses, particularly legacy signature-based security approaches.

Top Malware Detection


Sality.AN.gen
AdLoad.ACY
Virut.A_1064
SweetIM.A_6
Bredo.AIC_3
OptimumInstaller.A_2
Detected.A_151
Starter.C
AndroidOS.Agent.PI