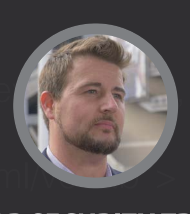
WatchGuard

2017 SECURITY PREDICTIONS

THE THREATS ARE REAL

2016 was a banner year for cyber attacks, featuring IoT botnets, crimeware-as-a-service and crypto ransomware. But as we move into 2017, what insidious events can we expect to grab headlines around the world? From Ransomworms to the first civilian casualties of the cyber cold war, read or watch WatchGuard's Chief Technology Officer, Corey Nachreiner, as he reports his threat predictions for the coming year.

OVERVIEW


TOP SECURITY TRENDS

SUMMARY OF PREDICTIONS

1 2017 will see the first ever Ransomworm, causing ransomware to spread faster.

Cyber criminals will take ransomware to the next level in 2017 by introducing the kind of auto-propagating characteristics traditionally found in network worms like CodeRed and Conficker. That's right, imagine a breed of ransomware designed to produce endless duplicates of itself, spreading the infection across an entire network. Whether you want to contemplate this scenario or not, it's only a matter of time before self-spreading ransomware – or ransomworms – begins to wreak havoc.

WATCH VIDEO

2 Attackers will exploit infrastructure-as-a-service (IaaS) as both an attack platform and attack surface.

Cloud adoption is growing at an incredible rate among organizations of all sizes. As these platforms have become increasingly engrained in the fabric of businesses' operations, they've also become a ripe target for criminal hackers. Public infrastructure-as-a-service (IaaS) will be leveraged as both a potential attack surface, and as a powerful platform to build criminals' malware and attack networks. Expect to see at least one headline-generating cyber attack either targeting or launched from a public IaaS service next year.

WATCH VIDEO

3 IoT devices become the de facto target for botnet zombies.

In 2016, the Mirai IoT botnet source code was leaked, enabling criminals to construct enormous botnets and launch gigantic distributed denial of service (DDoS) attacks with record-setting traffic. Now that hackers are weaponizing IoT devices in this way, we can expect them to expand beyond DDoS attacks in 2017. The pure volume of Internet-connected devices that are manufactured full of vulnerabilities presents a shiny new attack surface that hackers are sure to use to their advantage. In the coming year, we'll see criminals launch specialized IoT botnet click-jacking and spam campaigns to monetize these new attack methods the same way that traditional computer botnets were monetized.

WATCH VIDEO

4 In 2017, we'll see civilian "casualties" in the Cyber Cold War.

With the nation state cyber cold war well underway, expect to see at least one "civilian" casualty as collateral damage in 2017. In the past several years, nation states have allegedly damaged enemy nuclear centrifuges using malware, stolen intellectual property from private companies, and even breached other governments' confidential systems. For some time now, the U.S., Russia, Israel, and China have been mounting strategic cyber security operations and hording zero-day flaws to use against one another. This government practice of building up arsenals of vulnerabilities – rather than helping vendors fix them – will undoubtedly lead to an unsuspecting private business or citizen falling victim to an undisclosed zero-day exploit.

WATCH VIDEO

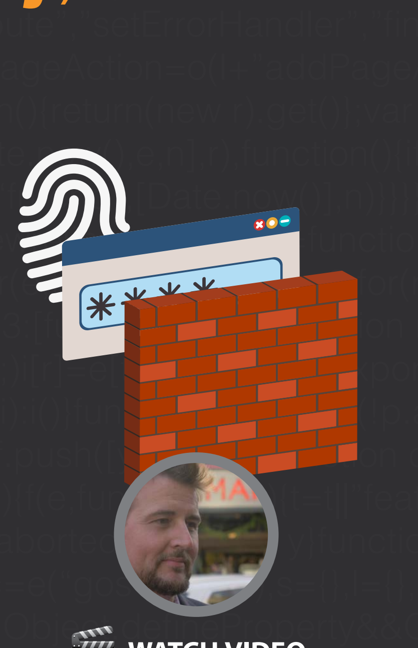
5 Under siege by cyber criminals, SMBs turn to small MSSPs for cyber security.

As they continue to be aggressively targeted by cyber criminals, small and medium businesses (SMBs) will continue to make network security a higher priority. With small IT teams and rarely any dedicated security professionals on staff, and without the resources to configure, monitor or adjust their own security controls, SMBs will recognize that their friendly neighborhood managed service provider (MSPs) may be the solution. As a result, MSPs will continue to add security services to their basic IT offerings. In 2017, at least a quarter of small businesses will turn to more specialized managed security services providers (MSSPs) for their security needs, and this percentage will continue to increase each year.

WATCH VIDEO

6 Increased biometrics usage hides continued credential insecurity; passwords aren't really gone.

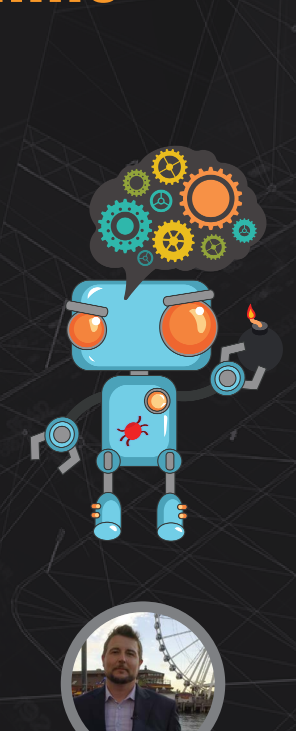
In the face of countless credentials breaches over the past several years, biometric solutions like fingerprint scanners for authentication will continue to rise as a popular alternative to passwords. These frequent breaches have also brought into question whether or not passwords should be part of the authentication solution at all. The widespread adoption of biometrics as a convenient alternative to remembering passwords, and as the primary method for authentication in 2017 will not erase the fact that weak passwords are still hiding in the shadows – a core part of operating systems and just as vulnerable as ever.



WATCH VIDEO

7 Attackers start leveraging machine learning and AI to improve malware and attacks.

Cyber security companies will come to a rude awakening when it becomes clear that they don't have a monopoly on machine learning in 2017. Machine learning has done far more than any human could to help the security industry become more predictive and less reactive in the fight against malware. By analyzing gigantic datasets and huge catalogs of good and bad files, these systems can recognize patterns that assist information security pros in rooting out never before seen threats. Next year, advanced cyber criminals will turn the tables and begin leveraging machine learning themselves to cook up new and improved malware to challenge machine learning defenses.



WATCH VIDEO

Cyber attacks will continue to be a major threat to businesses in 2017 and beyond. Staying educated on the latest infosec threats and solutions is the best way to improve your defenses.

Learn how WatchGuard can help defend your network today.

CLICK HERE

WatchGuard

© Copyright 2016 WatchGuard Technology, all rights resreved.