FORTINET

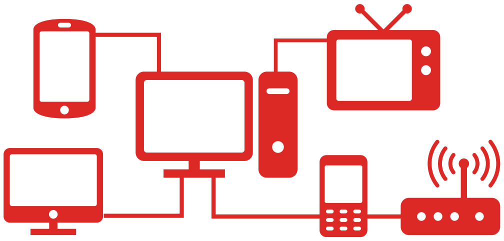
WHITE PAPER

New Rules:

The Evolving Threat Landscape in 2016

The threat landscape is in a constant state of evolution and the arms race between cyber guardians and cyber criminals has been heating up dramatically over the course of the last year. Over 20 billion devices are expected to be connected in the next four years alone, forcing individuals and organizations to face an exponentially expanding attack surface, bound to a borderless cyberspace. The consequences of falling behind in this arms race can be catastrophic and have elevated the discussion of cybersecurity to the boardroom. This is a complex scenario, and complexity is the enemy of security.

These predictions will provide an historical overview of the evolving threat landscape, reveal the new trends and strategies that Fortinet researchers anticipate cyber criminals will employ in the year to come, and demonstrate how Fortinet is proactively positioned to change the way businesses look at their security strategy going into the new year.



20 billion+

devices are expected to be connected in the next four years

Prediction #1: The Rise of Machine to Machine Attacks

The Threat: The exponential increase of unmanaged, “headless devices” driven by the Internet of Things will make these types of devices a tempting target for hackers looking to secure a beachhead into more traditional devices and corporate infrastructures. We will see a rise in the number of attacks that exploit flaws in trusted machine to machine (M2M) communication protocols.

Background:

- 2015 was the first year that IoT device attacks rose into FortiGuard’s top 10 threat list.
- Point of Sale (PoS) malware also entered the top 10 list in Japan.
- Researchers Miller and Valasek demonstrated flaws enabling them to compromise and control a connected vehicle in motion and estimate that there are 471,000 vehicles that could be vulnerable to attack.
- FortiGuard threat research has seen a significant increase in attacks that target connected consumer devices like IP Cameras.
- Gartner predicts that there will be more than 20 billion IoT devices by 2020.

Future Outlook:

- Exploits and malware will be developed that target trusted communication protocols and APIs: Bluetooth, RFID, NFC, Wi-Fi, Zigbee, etc.
- Land and Expand tactics start further away from defensive core as lucrative corporate networks implement better cyber defenses. Hackers will target devices further into their employees’ personal technology ecosystems to establish an initial beachhead.
- Connected medical devices and their host applications are a high-value target as the industry moves to adopt new technologies like medicine pumps, hospital bed sensors, smart blood pressure cuffs and others.
- Exploits in connected home automation devices like smart TVs, cameras, smart locks, lights, etc. will be used as an entryway into personal data and used as a vector to compromise corporate-issued devices. Home routers and networking continue to be highly targeted by hackers.

Prediction #2: Headless Worms Target Headless Devices

The Threat: Related to the rise in machine to machine attacks, the "headless devices" driven by the Internet of Things will also become a focus of worms and viruses that are designed to independently target and automatically propagate to other devices via trusted communication protocols. These viruses could be designed to cause the systematic failure of devices and the damages would be far more substantial as the numbers of IoT devices grows into the billions.

Background:

- 1971: The Creeper Virus was the first worm in history and was a proof of concept of a virus autonomously spreading through the TENEX Operating System.
- 1989: The Morris worm was designed to propagate through Unix operating systems and resulted in an estimated $100,000-$10,000,000 in damages. The first CERT team was established to combat this threat.
- Other notable worms: ILOVEYOU (2000), Anna Kournikova (2001), Slammer & Blaster (2003).
- There are various worms today that are designed to infect embedded devices such as home routers, but these have User Interfaces and connectivity features that allow them to be managed and infections remediated. Two examples of similar types of worms are "TheMoon" (2014) and "Moose" (2015) worms that exploit vulnerabilities in specific consumer routers.

Future Outlook:

- The Morris worm struck at a time where there were only 60,000 devices connected to the internet and estimates put the number of infected devices at around 6,000 or 10%. This number becomes far more substantial for popular devices like fitness trackers that currently have tens of millions of devices sold and in use.
- FortiGuard's research shows that it is possible to infect headless devices with small amounts of code. Exploits like these could lead to device to device propagation of worms, i.e. smartwatch to smartwatch malware, that spread through trusted communication protocols.

Prediction #3: Jailbreaking the Cloud

The Threat: As adoption of virtualization and cloud strategies increases, hackers are developing strategies to break out of hypervisors and infect the larger infrastructures and systems. Hackers will start targeting malware that exploits flaws in virtualization protocols to jailbreak the cloud and gain access to wider infrastructure data.

Background:

- As adoption of cloud and virtualization strategies increases, more and more systems are utilizing hypervisor processes to monitor code within end user environments.
- Known strategies to break out of the hypervisors have existed since vmftp in 2007, along with KVM Virtunoid in 2011 and others.
- 2015: A decade old vulnerability from 2004 known as Venom exploited floppy disk drivers to break out of a hypervisor and gain access to host operating systems.

Future Outlook:

- Cloud and virtualization adoption rates are increasing, making this the next big target for hackers looking to extract valuable corporate data and personal information.
- We expect to see malware in the wild that is designed to break out of hypervisors and gain access to host systems in order to infect wider corporate networks.
- Hackers may attempt to build malware into mobile application downloads for devices like smartphones and tablets that are used to remotely access virtual environments and resources.

Prediction #4: Ghostware Conceals Indicators of Compromise

The Threat: As cybercriminals become the focus of investigation and prosecution in the criminal justice system, careful hackers will develop a new variant of malware that is designed to achieve its mission and then erase all traces before security measures can detect that a compromise has taken place. FortiGuard predicts that we will witness Ghostware in 2016, written to steal data and disappear to conceal its creators.

Background:

- Criminal Justice agencies are doubling down on investigation, attribution and prosecution of the perpetrators of cybercrimes.
- Hackers will take a page from popular identity and content protection services like Snapchat, developing Ghostware that achieves a mission and then erases all traces of its existence.
- Fortinet predicted the rise of Blastware, first surfacing in the form of Rombertik, which performs checks once it has been installed to determine if it has been detected, self-destructing and permanently crashing the host system to avoid detection.

Future Outlook:

- New variants of Blastware will persist in targeted attacks, primarily utilized in acts of hacktivism or state-sponsored cybercrime.
- Ghostware will emerge that can exploit a system or infrastructure to extricate valuable data, then erase itself while leaving the host system intact.
- Ghostware attacks will enable hackers to cast a wider net for infection while attempting to avoid identification and attribution for the crimes.

Prediction #5: Two-Faced Malware

The Threat: Malware has been continually evolving features to avoid detection as security measure like sandboxing become more prevalent. As Sandboxing become more resistant to these countermeasures, we anticipate the development of Two-Faced Malware designed to execute an innocent task to avoid detection and then execute the malicious process once it has cleared security protocols.

Background:

- 2011: The Unitrix exploit executes various benign Unicode features to mask itself from detection engines.
- 2014: The Neutrino Botnet utilized various anti-detection strategies to avoid being discovered by antivirus and sandboxing features.
- Many sandbox solutions utilize a rating system based on the observed behavior of the files they are monitoring. If the sandboxes observe benign and typical behaviors, they will assign “innocent” ratings that can be reported back through a security vendor’s threat intelligence system. This could effectively enable an “all clear” that lets future versions of the files through deterrents like sandboxes.

Future Outlook:

- New malware will be written that employs multiple code execution paths that are designed to execute a benign process while under inspection and then execute its malicious process once clear.
- Two-faced Malware will be engineered to deliver counter threat intelligence and exploit the rating systems used by sandboxes and antivirus solutions. This counter threat intelligence can enable future variations of malware to bypass advanced security protection systems.
- These malware types will require stronger scrubbing and verification systems on the security vendor end. This could impact network performance and decrease the rate of adoption for more advanced security solutions.

About FortiGuard Labs

Knowledge of the threat landscape combined with the ability to respond quickly at multiple levels is the foundation of providing effective security. Since 2000, FortiGuard Labs have provided in-house, industry-leading security research on over 240 zero-day virus discoveries, powering Fortinet’s platform and suite of services.

FortiGuard takes information from global sources through its Security Services, using analytics and machine learning to turn big data into near real-time updates for Fortinet appliances, assuring some of the fastest response times in the industry to new vulnerabilities, attacks, viruses, botnets, and zero-day exploits.

FORTINET®

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

Nov 20, 2015