Weapons of Mass Disruption - Hackers in 2015

Presented by:
Universal Frameworks Inc.

UFI is your trusted partner in cyber security.

Visit us at www.universalframeworks.com

Contents

Trademark Names

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources UFI, considers to be reliable but is not warrantied by UFI.

Any product plans, specifications, and predictions herein are provided for information only and may be subject to change without warranty of any kind, express or implied.

This publication may contain opinions of UFI which are subject to change from time to time. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of UFI, is in violation of copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution.

Hacker's Tool Kits-

Advanced Attacks Mean Adopting New Threat Detection Techniques

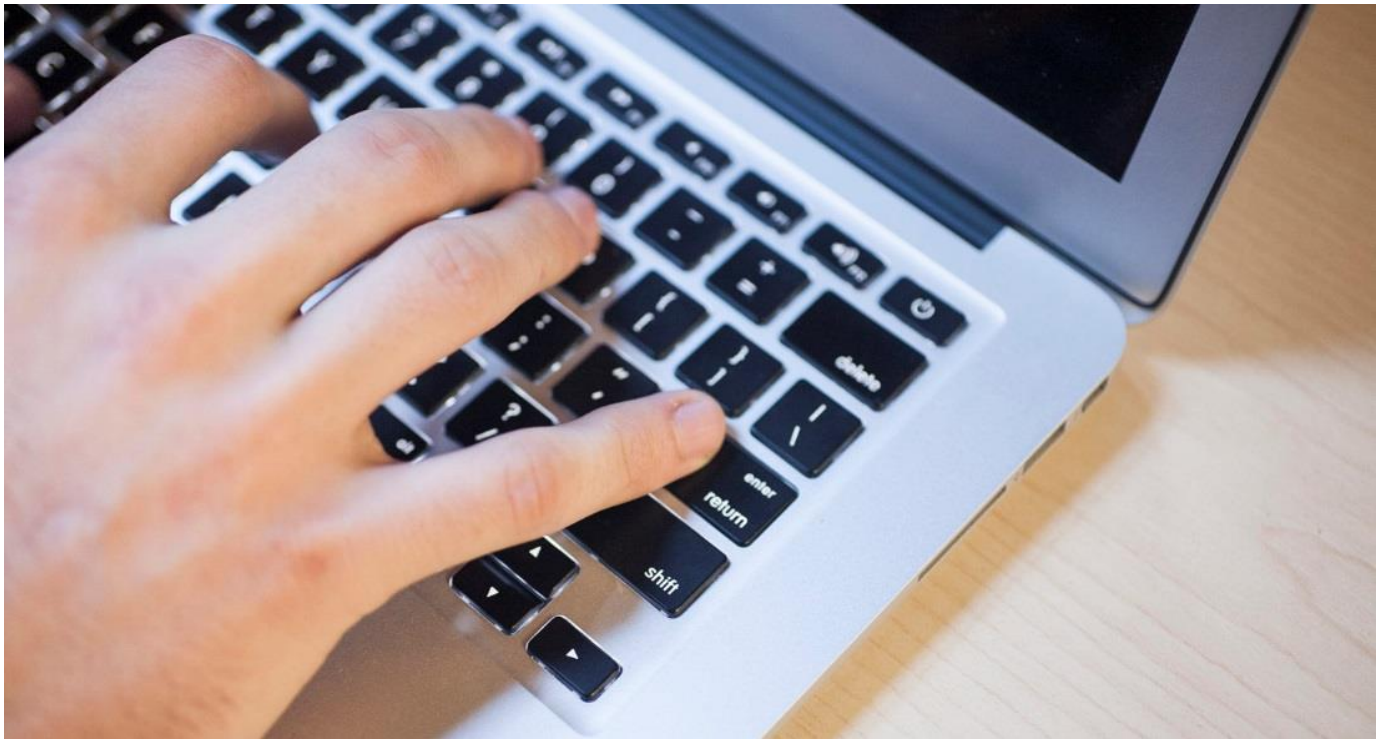
Attacks on an enterprise network have grown far beyond minor incidents into cybercriminals and highly skilled individuals executing advanced and intelligent attacks that can compromise sensitive corporate data. No longer can traditional malware-detection products suffice. Enterprises need advanced threat detection products and techniques to help protect their data.

Today's advanced malware and threat-detection products offered by various companies that aim to eliminate the problem of these new breeds of attacks. These advanced attacks combine sophisticated malware with the goal of taking sensitive enterprise data over a long period of time. This chapter will cover the advantages of these threat detection products as well as the challenges that they have not yet solved.

Next, the dramatic changes on the threat landscape which have grown over time, and how best to harden your network against targeted APT attacks. It explains why implementing a layered series of controls to achieve defense-in-depth network security is the best way to protect an enterprise network against APTs.

Lastly, Michael Cobb explores the evolution of threat detection and management. Specifically, he discusses the security vendors that are upgrading their intelligence-driven security products to stand up against today's advanced threats. Some of these include big data analytics, sandboxing and whitelisting.

Advanced Malware and Threat-Detection Products Emerge



Today's malware uses ingenious techniques to evade detection by traditional signature-based antimalware. IPS, Web filtering and antivirus products are simply no longer sufficient for defending against a new breed of attacker that combines sophisticated malware with persistent remote access, with the aim of stealing sensitive corporate data over an extended period of time.

New tools that offer advanced malware detection through sandboxing technology aim to counter this problem. These products are offered by various companies, including FireEye Inc, Damballa Inc, Palo Alto Networks, NetWitness and others. All of these systems promise near-complete protection from the malware threat. In this chapter, we'll discuss the emerging techniques employed by today's advanced malware and threat-detection products, focusing on the advantages they offer and the challenges that they have yet to solve.

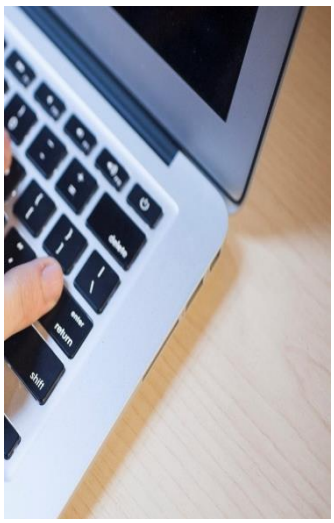
Advanced Malware and Threat-Detection Products Emerge

SANDBOXING TECHNOLOGY

The primary technique employed by a variety of advanced malware-detection products is known as sandboxing. With sandboxing, a potential malware threat is identified using various techniques. Network traffic analysis is used to discover potential threats on the network. Patterns of behavior are analyzed, and suspicious files are sent to the sandbox. The file is then examined in an environment of virtual machines that analyze behavior in a suite of different operating systems and software versions. All changes made by the file are recorded, and a report is presented which shows all areas of the operating system and software that were changed. Based on this report, the file can be flagged as malware.

The best aspect of this approach is that no matter the techniques used for hiding the payload of the malware, it still needs to affect the operating system in some way, and the sandboxing software will detect this. This two-stage process—first detecting the threat, and then passing it to the sandbox—significantly reduces false positives and false negatives.

Files are also analyzed at the point of entry into the network, for example when they are downloaded from a website. The Web traffic is reassembled by the product, and anomalies in the code are detected and assigned priority ratings. At a certain threshold, the suspicious traffic is passed to the sandbox. Threats already on the network are minimized by blocking data exfiltration attempts based on analysis of network traffic. The malware can be prevented from making callbacks, which is where the initial infection is then used to download further malware. Because it is not based on signatures, it can detect brand-new malware. Information on discovered malware is usually then shared among all of the devices, which enables quicker detection time for the threat.



Remote branch locations are often the starting point of attacks, and these locations need to be treated the same as any other part of the organization.

Advanced Malware and Threat-Detection Products Emerge

THREAT-DETECTION PRODUCT SELECTION

These tools are not cheap and careful consideration should be taken to ensure that the threat-detection system you choose is right for your organization. It is definitely worth investing the time in the free trials that some vendors offer in order to see if the system is valuable to your organization. It is important to note that once a product is chosen, it needs to be rolled out to all offices. Remote branch locations are often the starting point of attacks, and these locations need to be treated the same as any other part of the organization.

It is always important to remember that none of these products is a silver bullet. These systems cannot analyze SSL encrypted traffic, and, for the most part, they are only able to analyze threats against Windows environments. They are also unable to detect malware already installed on BYOD devices. However, the analysis of network traffic to prevent data exfiltration is a great feature to help counter some of these weaknesses.

Defense-in-depth is the key to preventing malware and APTs from penetrating your network and stealing secret and confidential data. These new technologies should be seen as one layer of the defense. They should be combined with an excellent team of incident-response specialists, and frequent penetration tests to simulate real-world attacks. Highly sophisticated adversaries will frequently attack you despite the defense these products offer. As these types of products become more popular, determined attackers will attempt to develop techniques to fool the software. It is one step in an arms race that will require organizations to invest in multiple layers of defense to keep their assets and sensitive data safe.

Defending the Network Against APT Attacks

The threat landscape has changed irrevocably. The primary foe of security professionals is no longer an asocial teenager basking in the glow of a monitor looking for an easy target, but rather the highly skilled technologists who are deliberately seeking treasure troves of sensitive information.

The change in landscape didn't happen suddenly. In 2006, we saw a highly targeted attack against the TJX Companies Inc. that resulted in the theft of personal information belonging to millions of individuals. In 2009, the Operation Aurora attacks saw Chinese sources infiltrating major American companies including Google Inc., Juniper Networks Inc. and Adobe Systems Inc.

. The following year, the Iranian government claimed that U.S. and Israeli interests were responsible for the Stuxnet worm attack on the Iranian nuclear program. And just last spring, RSA admitted it had been the victim of what it called "an extremely sophisticated cyber attack."

DEFINING AND UNDERSTANDING TARGETED APT ATTACKS

These attacks are representative of what security professionals face today. Aptly named advanced persistent threats, APT is a "fuzzy" and even controversial term that refers to a style of attack rather than any specific technique. Targeted APT attacks are waged in a one-to-one fashion by professional hackers using advanced skills.

While the "script kiddies" of yesteryear first selected a vulnerability and then scanned the Internet looking for systems susceptible to their chosen exploit, APT attackers first select their target—often a government agency, financial institution, corporate competitor or other high-value asset—and then probe for a method of entry.

Even though many information security industry observers bristle at the use of the term "advanced persistent threat" for a variety of reasons, it has become the most common phrase used to define this type of attack.

Coping with APTs requires security professionals to develop a new mindset. InfoSec pros must now assume attackers will successfully penetrate enterprise perimeters through dogged determination and the use of sophisticated tools. They will leverage zero-day attacks, social engineering, phishing and other techniques until they find a chink in our armor and gain a foothold on our network. Once they've established a virtual base of operations, they can escalate the privileges available to them and expand their scope of control until they achieve their objectives, even if it takes weeks or months for them to do so.

HARDENING THE NETWORK AGAINST TARGETED APT ATTACKS

Fortunately, there is a proven strategy for defending an enterprise network against APTs, and the good news is that it emphasizes many common network security best practices. The tried-and-true approach of implementing a layered series of controls to achieve defense-in-depth network security is the best way to protect an enterprise network against APTs.

First and foremost, take stock of the controls that already exist on the network and ensure they are both effective and well-managed. Most enterprises already have a mixture of firewalls, intrusion detection and prevention systems (IDS/IPS), antimalware packages and other controls. Are they audited regularly? Do they have current signatures? Are they consistently deployed? Check the basics before even considering adding additional layers of defense.

InfoSec pros must now assume attackers will successfully penetrate enterprise perimeters through dogged determination and the use of sophisticated tools.

Second, examine existing user education programs. Many APTs depend upon social engineering to exploit the poor security habits of users in other ways. For example, experts theorize that the Stuxnet worm penetrated the perimeter controls of an Iranian nuclear facility when it was carried into the secure facility by an authorized user on a flash drive. Make sure end users understand their role in protecting the security of the organization and that the organization has set clear expectations for user behavior.

DEFINING AND UNDERSTANDING TARGETED APT ATTACKS

HARDENING THE NETWORK AGAINST TARGETED APT ATTACKS

Using the threat of APT as a catalyst, this is a good time to evaluate existing network security controls and add additional safeguards, as necessary. After taking these remedial actions, consider the possibility of adding additional layers of defense to the network. There are three specific areas of control that are worthy of consideration:

- If a **Security Incident and Event Management (SIEM)** system isn't already in place, contemplate this as an opportunity to deploy one. SIEMs are a valuable tool in combating APTs because they consolidate and correlate security data from disparate sources. They can help identify the "needle in the haystack" that indicates a successful APT-style penetration of a network.

- **Data loss prevention** systems are an excellent last line of defense and may detect and block intentional or accidental attempts to remove sensitive information from a network.

Finally, **content filtering** provides the ability to further protect against phishing attacks and other Web- and email-borne threats. While user education is clearly the most comprehensive way to prevent successful social engineering, content filtering may catch users who have fallen victim to a solicitation before they compromise their accounts.

While it's true that APTs present a new type of threat to information security, they don't change the range of actions we must employ to protect ourselves. We simply need to return to the basics of defense-in-depth and layered controls that security professionals have been preaching for years.

Advanced Attacks Call for Sophisticated Threat Detection Products

Cybercriminals of all persuasions now easily and routinely bypass existing enterprise security defenses by blending into the background noise of an organization's operations. These advanced attacks now take place over months and years, subverting traditional malware-detection products that only scan for known malware at a given point in time.

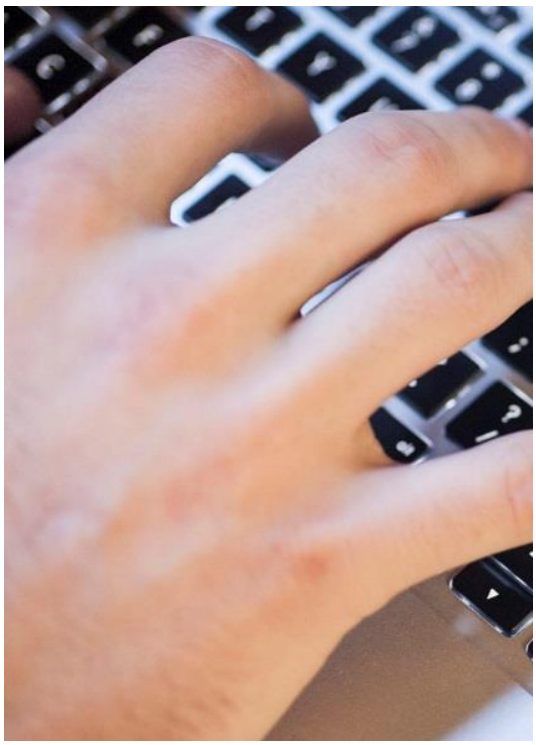
For example, a newly discovered Trojan called APT. BaneChant uses multiple detection-evasion techniques, including masquerading as a legitimate process, monitoring mouse clicks to avoid sandbox analysis and performing multi-byte XOR encryption to evade network-level binary extraction technology. It also uses fileless malicious code loaded directly into memory and escapes automated domain blacklisting by using redirection via URL shortening and dynamic DNS services.

Such attacks are testing the limitations of existing security analytics tools, and the recent Mandiant Corp. APT1 report shows just how long-running and sophisticated cyberespionage campaigns have become. According to the 2013 Cyber Threat Readiness survey conducted by LogRhythm, an alarming 75% of respondents lack confidence in their ability to recognize key indicators of a breach.

Many reported breaches have originally gone undetected with most discovered not by the in-house security team, but by a third party.

Enterprises can no longer rely solely on endpoints to stop this type of malware infection. Additional dynamic before-the-fact defenses must be implemented to effectively combat advanced attacks at all layers and identify behaviors not seen before. Thankfully many security vendors are starting to upgrade their intelligence-driven security products to counter the problem of today's advanced threats.

BIG DATA ANALYTICS



One common approach is the incorporation of security big data analytics to aid the discovery of malicious activity hidden deep in the masses of an organization's network traffic. Big data is defined as any type of data, structured and unstructured, that can provide insight into network activity.

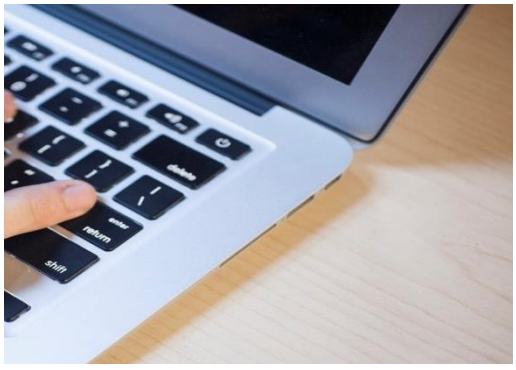
Other system information, such as processor or memory utilization, can highlight unexpected changes in the status of a system while external threat intelligence feeds can further clarify what's normal or acceptable by not limiting analysis to just the data created by one organization. While this data has for years been stored in siloed repositories or disparately throughout an enterprise, the dire realities of today's attack landscape have fostered new demand for technology that can aggregate this data, analyze it quickly and develop clues pointing to advanced attacks that would otherwise go undetected.

Although security information and event management (SIEM) products offer a central point of collection and monitoring for enterprise activity data, they have been mainly deployed in order to meet compliance reporting requirements, particularly with the merchant-focused Payment Card Industry Data Security Standard (PCI DSS). Few organizations actually use the technology's event-correlation capabilities and most products don't provide enough in-depth visibility to facilitate today's analytic needs. Vendors are seeking to address this with next-generation SIEM products that widen the scope and scale of data collection and real-time analysis so that diverse events can be put into context to find unusual activity.

BIG DATA ANALYTICS

•(It should be noted that network behavioral anomaly detection (NBAD) products do provide this capability, but only at the network layer.)

•Real-time analysis using adaptive intelligence of this big data—understanding what's normal in order to recognize what's abnormal—can greatly improve the chances of recognizing the indicators of an advanced threat or breach from numerous attack vectors such as advanced persistent threats, fraud and malicious insiders. This pre-attack focus aims to keep a network ahead of attackers and pinpoint potential attack patterns, even if they are spread out over a period of time.



There are plenty of new innovative products coming onto the market. The LogRhythm SIEM 2.0 platform now integrates with Rapid7's Nexpose vulnerability management product to deliver data security analytics and unified risk assessment capabilities from within the LogRhythm console. IBM is combining security intelligence with big data using the IBM QRadar Security Intelligence and IBM Big Data Platforms to provide a comprehensive, integrated approach to real-time analytics across massive structured and unstructured data. The RSA Security Analytics product uses threat intelligence from the global security community and RSA FirstWatch to leverage what others have already uncovered and improve detection of malicious activity within an organization's big data.

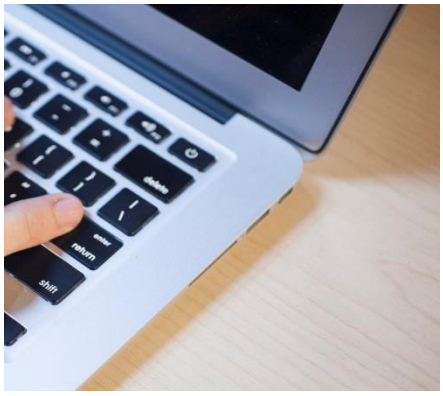
Scalability, powerful analytical tools, and support for heterogeneous event sources are the most important capabilities when assessing next-generation SIEM products, particularly when it comes to time-sensitive processes such as fraud detection, to ensure that they can process the vast amounts of diverse data. Certainly check that any shortlisted solution creates actionable intelligence based on business context so threats which pose the greatest risk are prioritized. Tools for visualizing and exploring big data are another key feature as they can quickly highlight infected devices and other hot spots.

BIG DATA ANALYTICS

SANDBOXING AND WHITELISITING

SIEM and big data are not the only options when it comes to mitigating today's threats. Sandboxing and whitelisting are other technologies worth considering. Bit9's whitelist security software is a trust-based solution using endpoint agents that allows administrators to specify software that can execute on desktops and laptops. A new feature is the ability to leverage the on-demand cloud-based Bit9 Software Reputation Service for highly accurate detection of suspicious malware and associated files.

Enterprises running their own app stores can also use the Lookout API to ensure that the apps offered are safe.



Sandboxing keeps applications separate so malicious code cannot transfer from one process to another. Any application or content that is unknown can be treated as untrusted and isolated in its own sandbox. McAfee, like other security vendors, has been acquiring relevant technologies to add to its product range. It plans to offer sandboxing technology in its ePolicy Orchestrator suite in the second half of 2013. By running suspected malware in a sandbox, it can learn what effect it will have on an endpoint and automatically block future occurrences and remediate any already infected endpoints. Fortinet's FortiCloud cloud-based sandboxing service provides an online sandboxing portal to execute suspicious code in a virtual environment.

BIG DATA ANALYTICS – Sandboxing and Whitelisting

Of course, security teams need to extend threat detection and protection to the mobile devices connecting to their networks, particularly as mobile device users are at least three times more likely to become victims of phishing attacks than desktop users.

The Mobile Threat Network from Lookout Mobile Security delivers over-the-air protection to mobile users. Lookout is another product that uses a big data analysis approach for spotting malware and predicting where it will crop up next. Enterprises running their own app stores can also use the Lookout API to ensure that the apps offered are safe. The RSA Fraud Action Anti Rogue App Service also detects any malicious or unauthorized mobile apps that infiltrate online app stores.

Whichever advanced threat detection technology an organization deploys, its effectiveness will depend on those configuring and monitoring it.

People are always going to be a big part of any threat management program. Administrators must learn how to use emerging technology effectively so that it actually provides additional protection. Training such as Symantec's Cyber Threat Detection and Incident Response Training as well as the many in-depth training courses provided by SANS and others will help staff understand how to identify threats and respond and recover from malicious events.

As with any new IT technology, it's important not to get caught up in vendors' marketing hype. Concentrating more on detection and response doesn't mean that point defense technologies like firewalls and antivirus are no longer relevant. Securing any network will still require documented policies and procedures as a foundation for success. Classification of assets and data is essential and remember that although threat management begins with threat identification, remediation is also an essential part of a successful threat management process.

Who we are:

Mechelen based, Universal Frameworks Inc., (UFI) systems, is an IT driven cyber security company whose team approach creates cyber security products and services that utilize Key Enabling Technologies (KETs) - specifically in the areas of ICT, and ICS.

We are dedicated to being the premier global developer and the dominant source in the cyber security industry for ICT and ICS.

We accomplish this through building long term committed relationships with our: clients, partners, vendors, employees and all stakeholders.

UFI overcomes some of the most challenging cyber security and information technology problems facing our clients today.

UFI works with its clients and provides an always-on user experience through fast, secure delivery of dynamic connected cyber security frameworks, technologies and services.

Through actionable insights that accelerate, monitor, and secure application and service delivery, UFI's clients benefit from faster time to market, optimized application performance, and higher-quality deployments.

"UFI-Your trusted partner in cyber security."

Visit us at www.universalframeworks.com