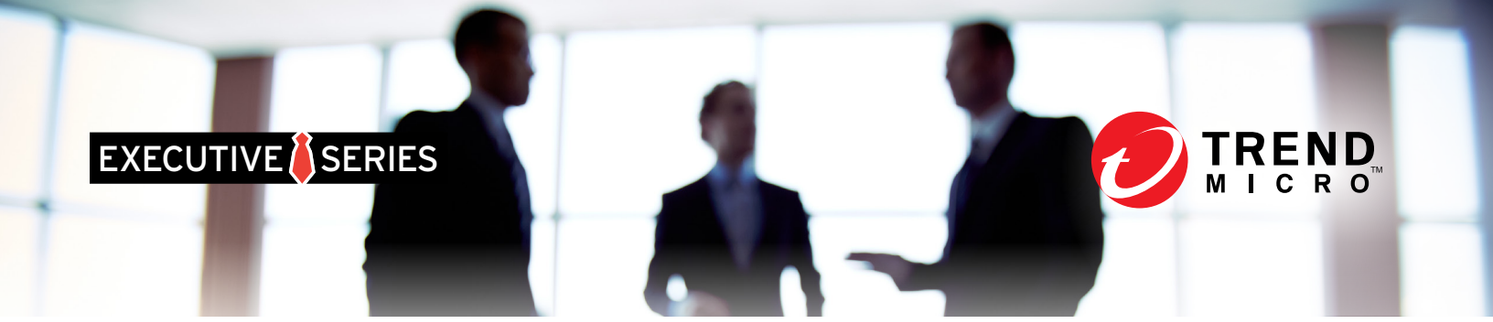

Exploits as a Service

Cybercrime-as-a-Service Series

Cybercrime as a service (CaaS) is an important trend in Deep Web forums because it puts cybercriminal tools and services in the hands of a wider range of threat actors—even the nontechnical, such that anyone can become a cybercriminal with minimal investment. At the same time, cybercriminals are now seeing the advantages of expanding their targets from home users to larger enterprise networks. This is a matter that IT administrators need to be ready for.

Exploit Kits

The first exploit kit found in the cybercriminal underground, WebAttacker, appeared in 2006 and pooled exploits for vulnerabilities in common PC software, while providing the end-to-end infrastructure for the attack chain.[1] Unlike more standardized goods such as stolen personally identifiable information (PII), however, exploit kits are sold in forums instead of marketplaces.[2]

In true open-market style, criminal developers soon figured out that specialization led to better efficiency and greater profit. As hackers focus on specific aspects of a typical attacker infrastructure, other cybercriminals can pick and choose which tasks to automate and customize.

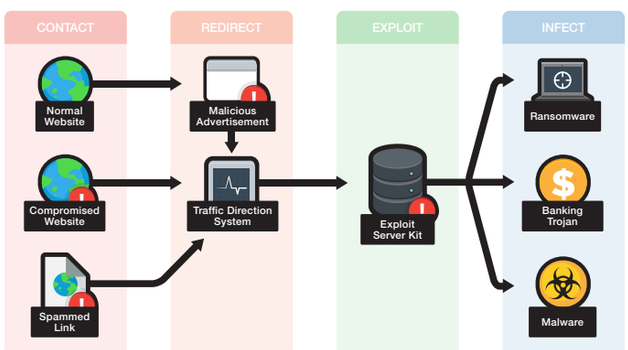

Figure 1. Typical exploit kit attack chain[3]

One aspect of malware campaigns that is difficult for nonexperts to get in to, but reaps incredible benefits for fledgling cybercriminals because of its likelihood to succeed, is exploit creation and delivery. Exploits lessen the number of user clicks required to infect a system because they typically take advantage of flaws in software that allow them to execute arbitrary code. This makes exploits a key ingredient in drive-by downloads, malvertisements, watering-hole attacks and even the more insidious targeted attacks.

> More than **100 exploits** have been integrated into 70 exploit kits in 2014.

Software vendors typically patch a vulnerability when they know it is actively being exploited in the wild. Therefore, a cybercriminal service that exclusively focuses on ensuring that the exploitation process is reliable and covers as many new exploits for even the most up-to-date systems, will go for a good price. This service is embodied in today's modern exploit kits, which go as far as being rentable by the hour, as their creators take care of exploit creation and hosting.

> Exploit kits can be rented by the hour, day, or month. When Angler started taking a dip, Neutrino jacked up its price by 100% from **US$3,500 to US$7,000** per month.[4]

Exploit Kit + Ransomware Power Combo

Still one of the most widespread and dreaded malware types is ransomware—malware that let criminals hold a system's files hostage in exchange for money.

In 2015, Angler started delivering ransomware. As each leg of the cybercriminal operation became better at fulfilling its purpose, the likelier it became for more users to face their own fight with ransomware.

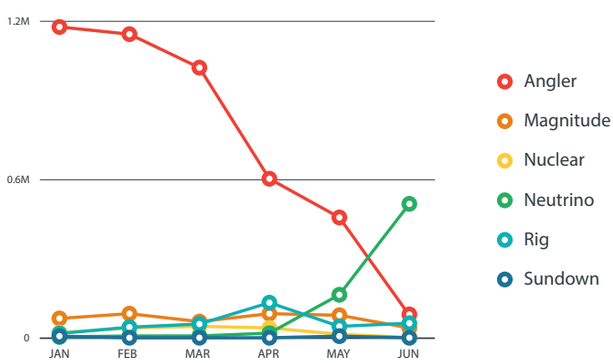

Figure 2. Number of times exploit-kit-hosting URLs were accessed in the first half of 2016

Throughout the years, exploit kits came and went, but the successful ones became much faster at integrating new software vulnerabilities and much better at applying various evasion techniques compared with competing services.

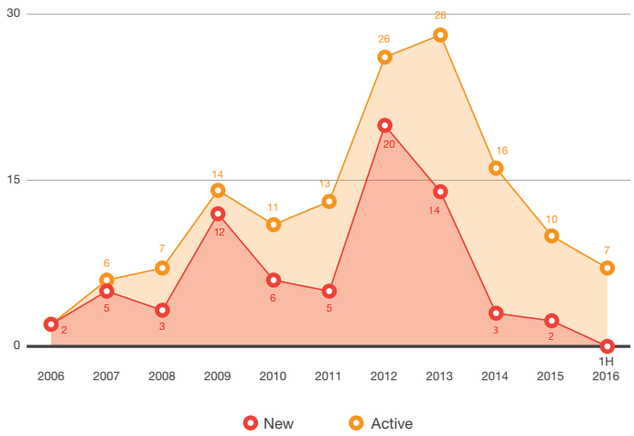

Figure 3. Active versus new exploit kits from 2006 to the first half of 2016

What This Means for Enterprises

Trend Micro (with TippingPoint) and the Zero Day Initiative (ZDI) discovered and/or disclosed a total of 473 vulnerabilities in the first half of 2016 alone.[4] The greatest number of vulnerabilities was found in Adobe® Flash® Player, one of the most ubiquitous pieces of software in modern systems.

> Adobe Flash, the software most often targeted by exploit kits, is installed in more than **1B connected systems** to date.

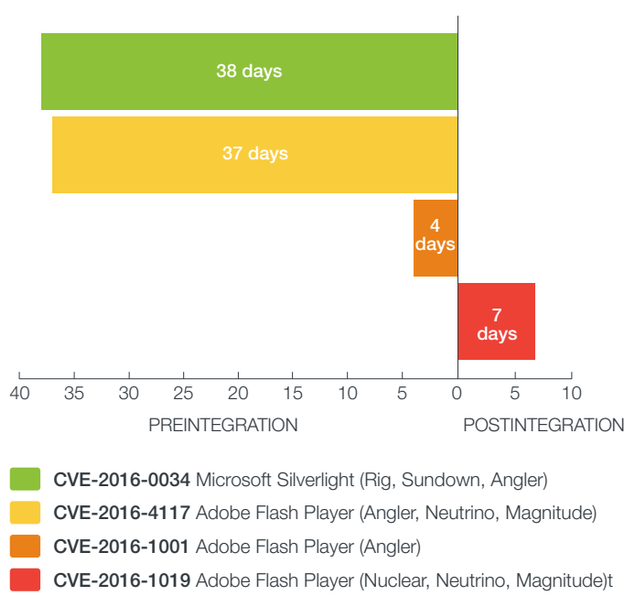

Figure 4. Windows of exposure tied to exploits that were integrated into kits in the first half of 2016

Because exploit kits are quick to integrate zero-day vulnerabilities as they play cat and mouse with software vendors, enterprises continue to risk encountering threats to their networks.

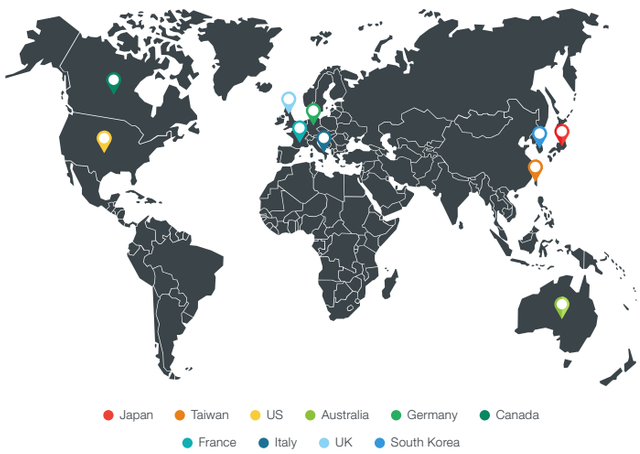

Figure 5. Over 80% of individuals who clicked exploit-kit-related URLs in the second quarter of 2016 came from these 10 countries

As cybercriminals continue to use the deadly exploit-kit-ransomware combination, enterprises must contend with the risks of ransomware infection, along with any other new-fangled malware exploit kit operators decide to deliver.

Exploit Kit	Ransomware Delivered	
	2015	2016
Angler	CRILOCK (CryptoLocker)	CRILOCK (CryptoLocker)
	CRYPTESLA (TeslaCrypt)	CRYPTESLA (TeslaCrypt)
	CRYPWALL (CryptoWall)	CRYPWALL (CryptoWall)
		WALTRIX (CryptXXX)
Neutrino	CRYPTESLA (TeslaCrypt)	CERBER
	CRYPWALL (CryptoWall)	CRYPTESLA (TeslaCrypt)
		CRYPWALL (CryptoWall)
		LOCKY
		WALTRIX (CryptXXX)
Magnitude	CRYPWALL (CryptoWall)	CERBER
		CRYPWALL (CryptoWall)
Rig	CRYPTESLA (TeslaCrypt)	CERBER
	CRYPWALL (CryptoWall)	GOOPIC
Nuclear	CRYPCTB (Cryptroni/ Critroni/CTB-Locker/ Curve-Tor-Bitcoin Locker	CRYPTESLA (TeslaCrypt)
	CRYPSHED (Troldesh)	LOCKY
	CRYPTESLA (TeslaCrypt)	
	CRYPWALL (CryptoWall)	
Sundown		CRYPTOSHOCKER
Hunter		LOCKY
Fiesta	CRYPTESLA (TeslaCrypt)	

Table 1. Ransomware families delivered by exploit kits

In ransomware's case, data loss is an imminent risk, along with other direct and indirect effects to a company's bottom line in terms of:

- Lost sales
- Payment, delivery, or transaction delays
- Unfulfilled orders
- Business process disruption
- Productivity losses
- Legal fines
- Regulatory penalties
- Damage to brand and reputation

What Enterprises Can Do

Vulnerabilities that can be patched should be at the soonest possible time, whether they are in database applications or browser plug-ins. This policy is basic for network defenders, and should be considered a critical security task.

The nature of businesses, however, does not allow impromptu system downtimes for patching. Certain legacy, in-house developed, or no-longer-supported software will also never be patched. Temporarily shielding endpoints via Intrusion Prevention System (IPS) filters is an enterprise's next best option.

Modern data centers have evolved to use a mix of physical, virtual, and cloud platforms, so a company's security strategy should be able to adapt and be controllable from a single console.

Trend Micro understands the value of analyzing the entire attack chain—from entry points such as malicious URLs and spam and the use of exploits and various evasion techniques to the phone-home communication back to operators—and strengthening the ability to block malware before they execute on systems.[6, 7]

As network defenders scale up to protect hundreds to thousands of endpoints, different layers of protection must be able to "talk to each other," forming a connected threat defense strategy. All layers must have access to threat intelligence, security updates, and protection afforded by security technologies such as:

- Advanced anti-malware (beyond blacklisting)
- Antispam at the Web and messaging gateways
- Web reputation
- Application control (whitelisting)
- Content filtering
- Vulnerability shielding
- Mobile app reputation
- Intrusion prevention
- Host-based firewall protection

A majority of today's threats can be detected by the aforementioned techniques working together, but vulnerabilities will continue to be found before vendors can patch them, so enterprises must finally be able to catch zero-day and "unknown" threats through behavior and integrity monitoring as well as sandboxing.

Machine learning, in particular, can identify exploit kit activity through repeated exposure to human- or computer-provided input to compute a mathematical model. By "training" a security product, networks are defended in real time against even hard-to-detect threat components such as exploit kits.

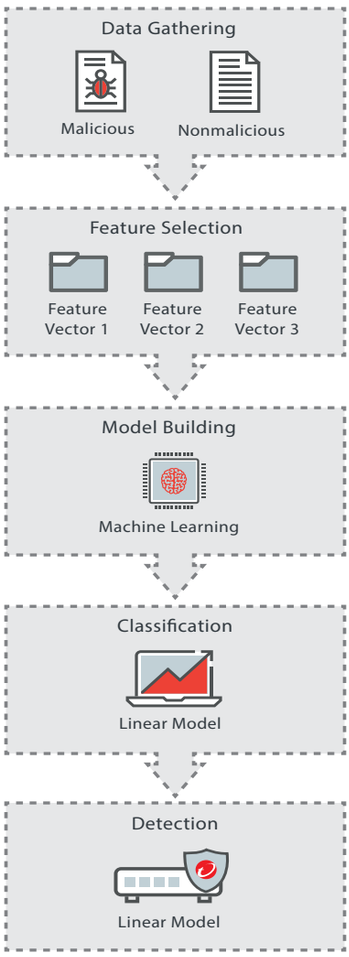

Figure 6. How machine learning works to protect against vulnerability exploits

References:

1 https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits.pdf

2 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/wp-russian-underground-2.0.pdf

3 http://www.trendmicro.com/vinfo/us/security/definition/Exploit-Kit

4 http://malware.dontneedcoffee.com/2016/06/is-it-end-of-angler.html

5 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-the-reign-of-ransomware.pdf

6 http://www.trendmicro.com/us/enterprise/product-security/vulnerability-protection/

7 http://www.trendmicro.com/us/business/network-security/