RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SPO3-R04

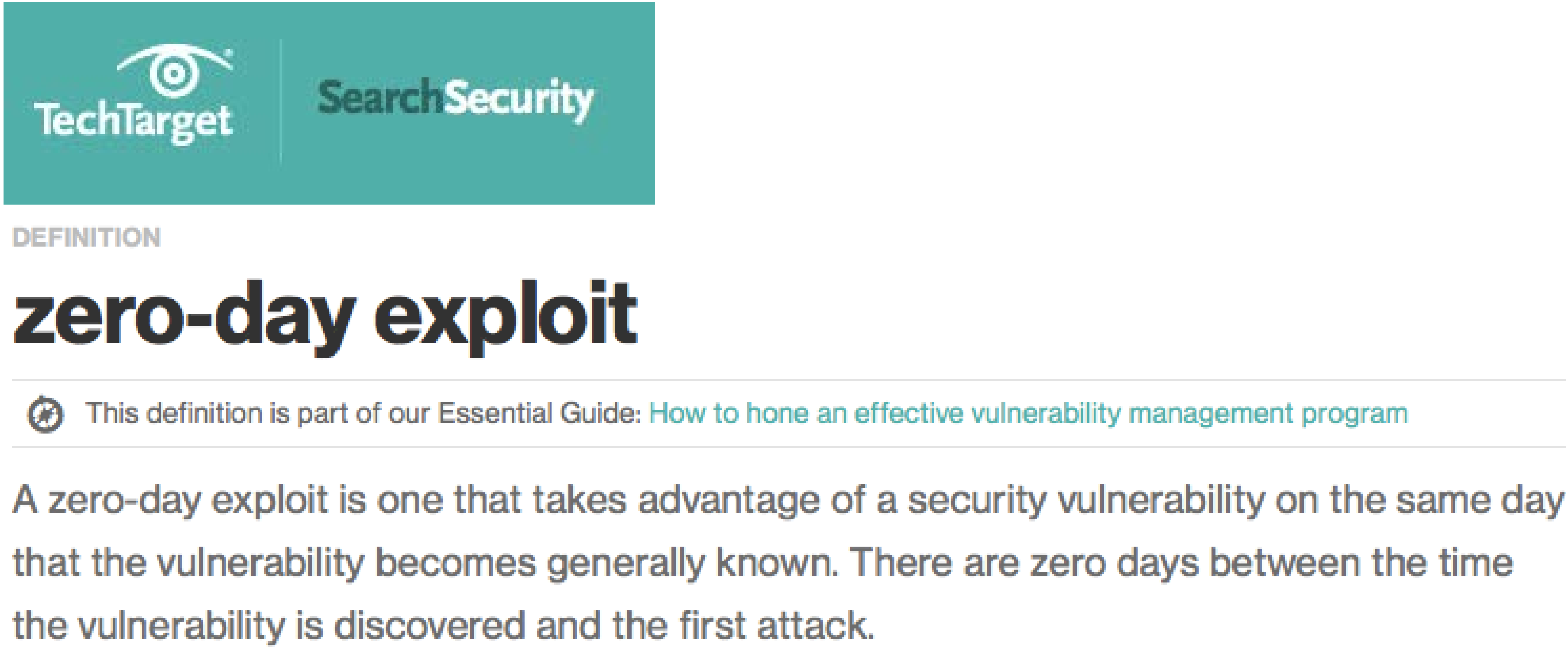
The Virtual Patching of Zero-Day Vulnerabilities

Raimund Genes

CTO
Trend Micro

#RSAC

Zero Days?



TechTarget | SearchSecurity

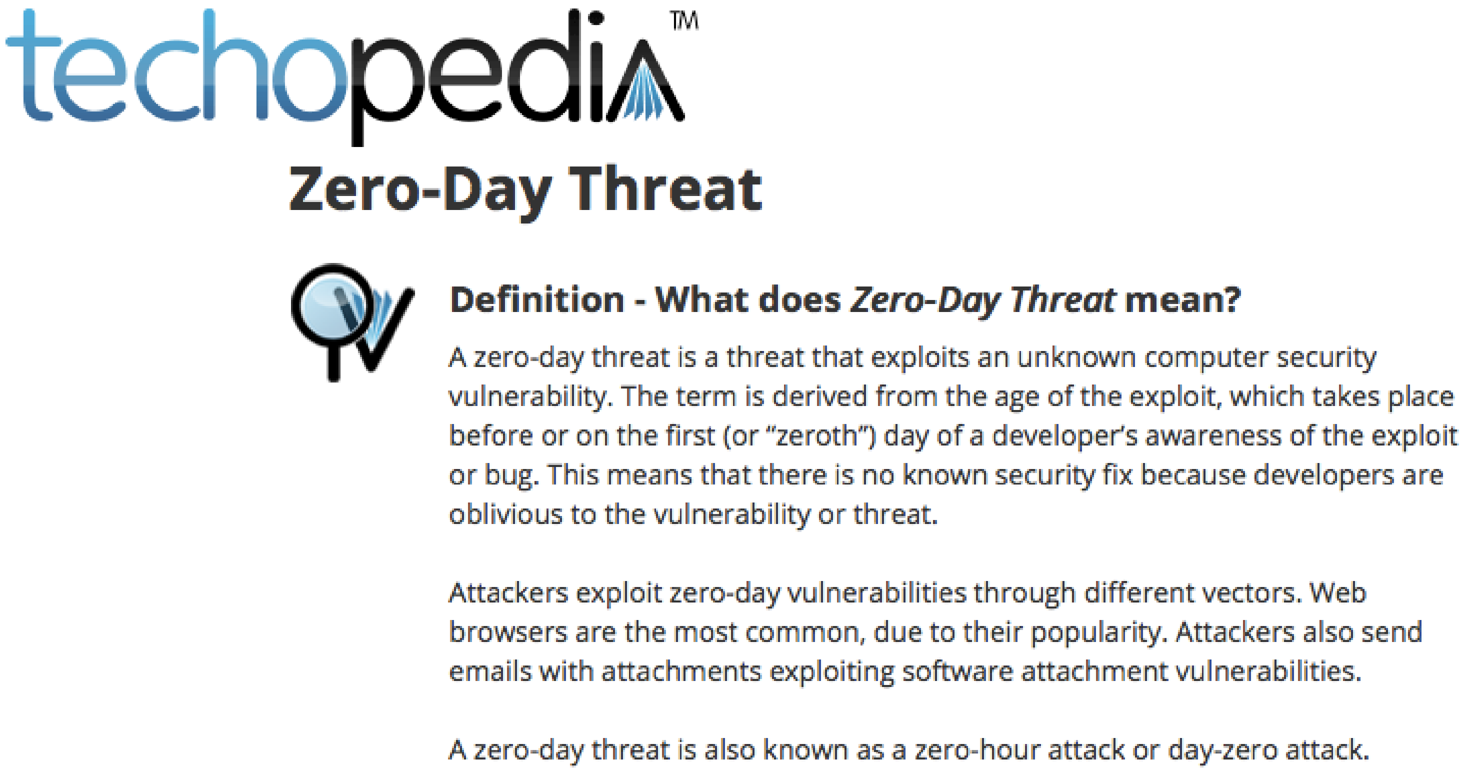
DEFINITION

zero-day exploit

This definition is part of our Essential Guide: How to hone an effective vulnerability management program

A zero-day exploit is one that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known. There are zero days between the time the vulnerability is discovered and the first attack.

Zero Days?



techopedia™

Zero-Day Threat

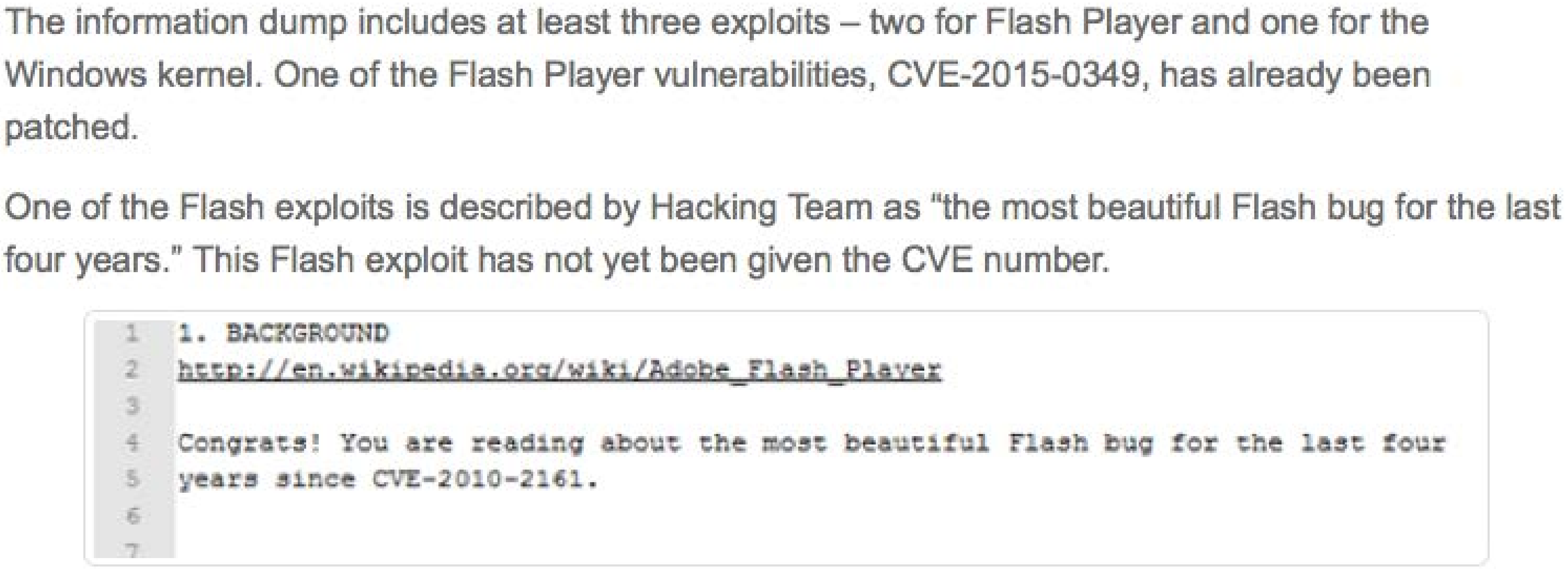
Definition - What does *Zero-Day Threat* mean?

A zero-day threat is a threat that exploits an unknown computer security vulnerability. The term is derived from the age of the exploit, which takes place before or on the first (or "zeroth") day of a developer's awareness of the exploit or bug. This means that there is no known security fix because developers are oblivious to the vulnerability or threat.

Attackers exploit zero-day vulnerabilities through different vectors. Web browsers are the most common, due to their popularity. Attackers also send emails with attachments exploiting software attachment vulnerabilities.

A zero-day threat is also known as a zero-hour attack or day-zero attack.

Trend Micro blog entry from 7th of July 15



The information dump includes at least three exploits – two for Flash Player and one for the Windows kernel. One of the Flash Player vulnerabilities, CVE-2015-0349, has already been patched.

One of the Flash exploits is described by Hacking Team as “the most beautiful Flash bug for the last four years.” This Flash exploit has not yet been given the CVE number.

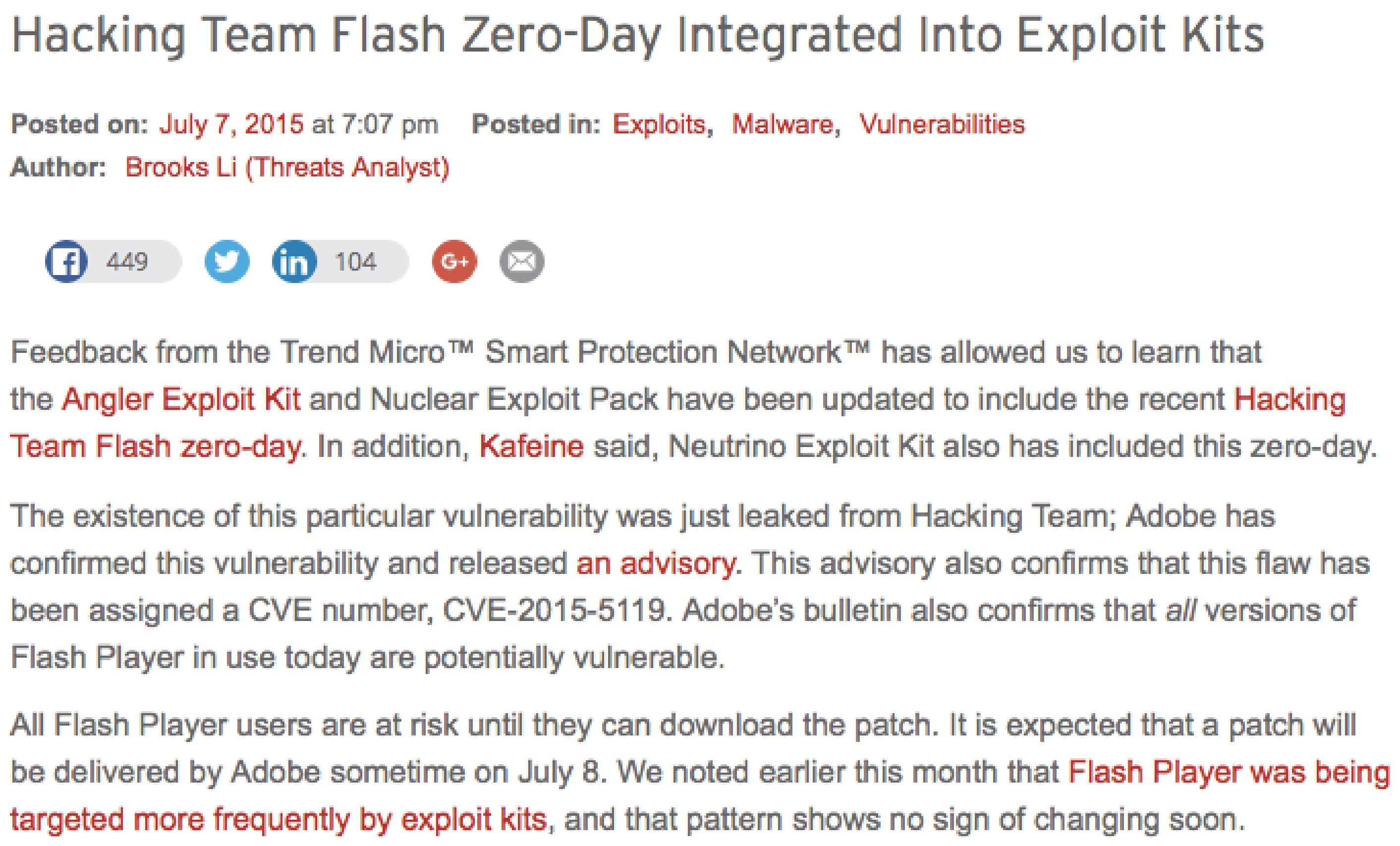
```
1. BACKGROUND
http://en.wikipedia.org/wiki/Adobe_Flash_Player

Congrats! You are reading about the most beautiful Flash bug for the last four
years since CVE-2010-2161.


```

Figure 1. Description of vulnerability by Hacking Team

Zero Days?



Hacking Team Flash Zero-Day Integrated Into Exploit Kits

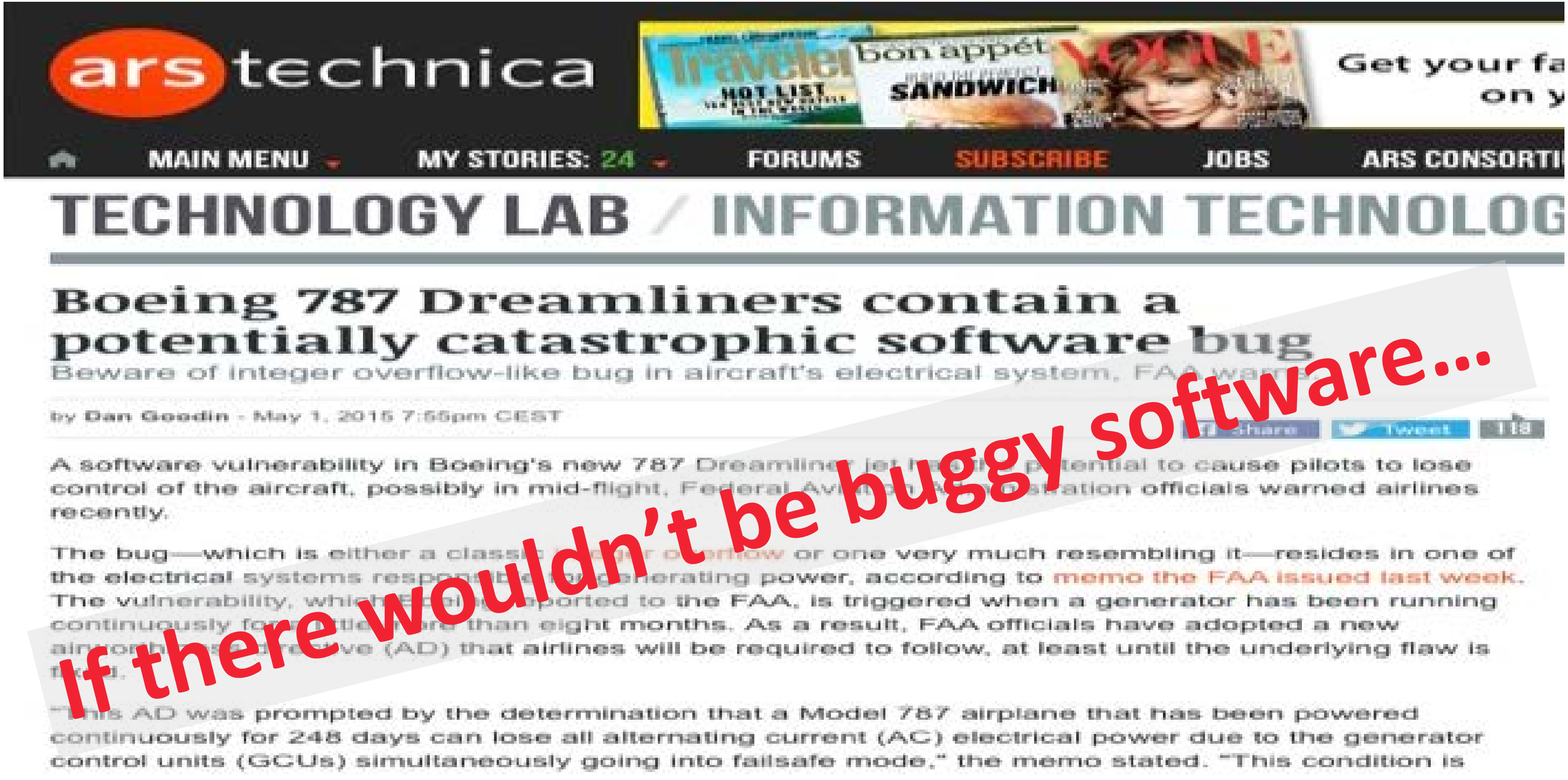
Posted on: July 7, 2015 at 7:07 pm **Posted in:** Exploits, Malware, Vulnerabilities
Author: Brooks Li (Threats Analyst)

Feedback from the Trend Micro™ Smart Protection Network™ has allowed us to learn that the Angler Exploit Kit and Nuclear Exploit Pack have been updated to include the recent Hacking Team Flash zero-day. In addition, Kafeine said, Neutrino Exploit Kit also has included this zero-day.

The existence of this particular vulnerability was just leaked from Hacking Team; Adobe has confirmed this vulnerability and released an advisory. This advisory also confirms that this flaw has been assigned a CVE number, CVE-2015-5119. Adobe's bulletin also confirms that *all* versions of Flash Player in use today are potentially vulnerable.

All Flash Player users are at risk until they can download the patch. It is expected that a patch will be delivered by Adobe sometime on July 8. We noted earlier this month that Flash Player was being targeted more frequently by exploit kits, and that pattern shows no sign of changing soon.

So who’s behind all these zero days?



Boeing 787 Dreamliners contain a potentially catastrophic software bug

Beware of integer overflow-like bug in aircraft's electrical system, FAA warns

by Dan Goodin - May 1, 2015 7:55pm CEST

A software vulnerability in Boeing's new 787 Dreamliner jet has the potential to cause pilots to lose control of the aircraft, possibly in mid-flight, Federal Aviation Administration officials warned airlines recently.

The bug—which is either a classic integer overflow or one very much resembling it—resides in one of the electrical systems responsible for generating power, according to memo the FAA issued last week. The vulnerability, which Boeing reported to the FAA, is triggered when a generator has been running continuously for a little more than eight months. As a result, FAA officials have adopted a new airworthiness directive (AD) that airlines will be required to follow, at least until the underlying flaw is fixed.

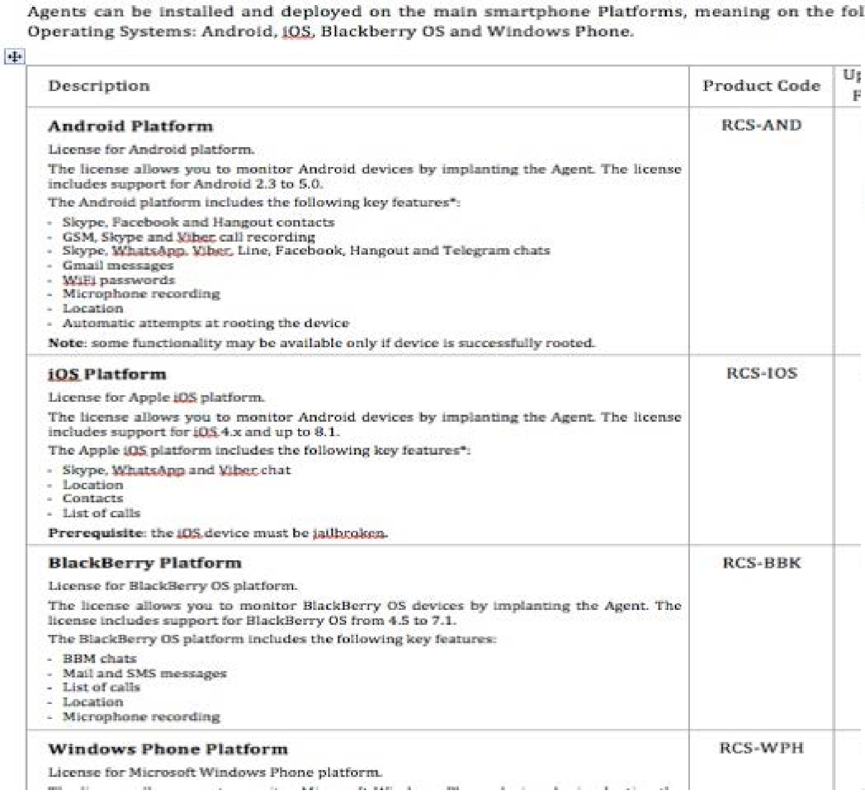
"This AD was prompted by the determination that a Model 787 airplane that has been powered continuously for 248 days can lose all alternating current (AC) electrical power due to the generator control units (GCUs) simultaneously going into failsafe mode," the memo stated. "This condition is

If there wouldn’t be buggy software…

Government contractors

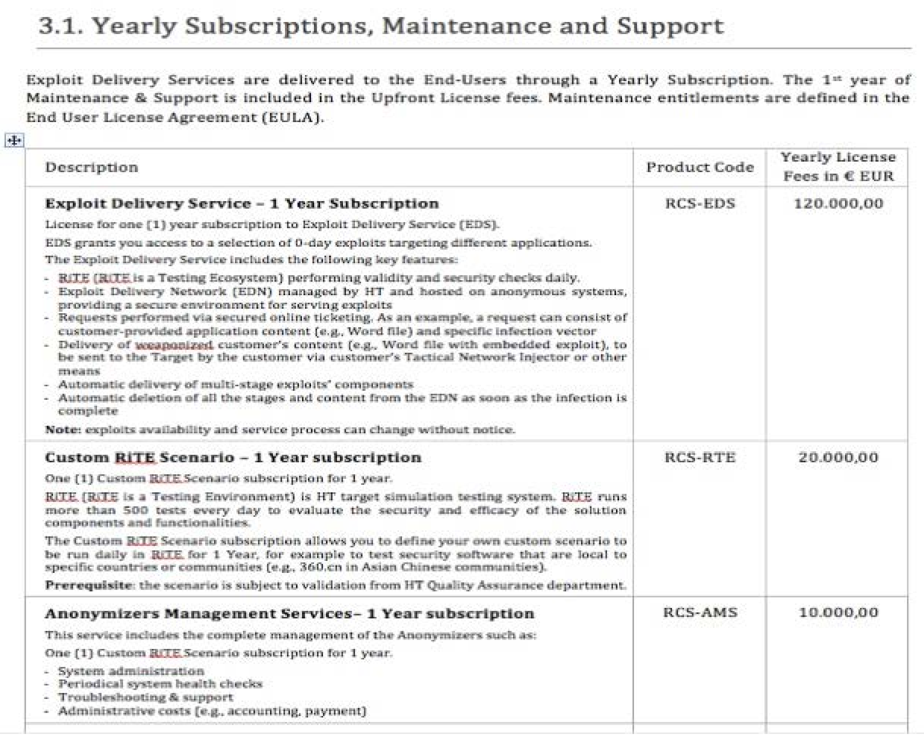
HackingTeam

Remote Control System
Price Scheme



Agents can be installed and deployed on the main smartphone Platforms, meaning on the following mobile Operating Systems: Android, iOS, Blackberry OS and Windows Phone.

Description	Product Code	Up F
Android Platform License for Android platform. The license allows you to monitor Android devices by implanting the Agent. The license includes support for Android 2.3 to 5.0. The Android platform includes the following key features*: - Skype, Facebook and Hangout contacts - GSM, Skype and Viber call recording - Skype, WhatsApp, Viber, Line, Facebook, Hangout and Telegram chats - Gmail messages - WiFi passwords - Microphone recording - Location - Automatic attempts at rooting the device **Note**: some functionality may be available only if device is successfully rooted.	RCS-AND	
iOS Platform License for Apple iOS platform. The license allows you to monitor Android devices by implanting the Agent. The license includes support for iOS 4.x and up to 8.1. The Apple iOS platform includes the following key features*: - Skype, WhatsApp and Viber chat - Location - Contacts - List of calls **Prerequisite**: the iOS device must be jailbroken.	RCS-IOS	
BlackBerry Platform License for BlackBerry OS platform. The license allows you to monitor BlackBerry OS devices by implanting the Agent. The license includes support for BlackBerry OS from 4.5 to 7.1. The BlackBerry OS platform includes the following key features: - BBM chats - Mail and SMS messages - List of calls - Location - Microphone recording	RCS-BBK	
Windows Phone Platform License for Microsoft Windows Phone platform.	RCS-WPH	



3.1. Yearly Subscriptions, Maintenance and Support

Exploit Delivery Services are delivered to the End-Users through a Yearly Subscription. The 1st year of Maintenance & Support is included in the Upfront License fees. Maintenance entitlements are defined in the End User License Agreement (EULA).

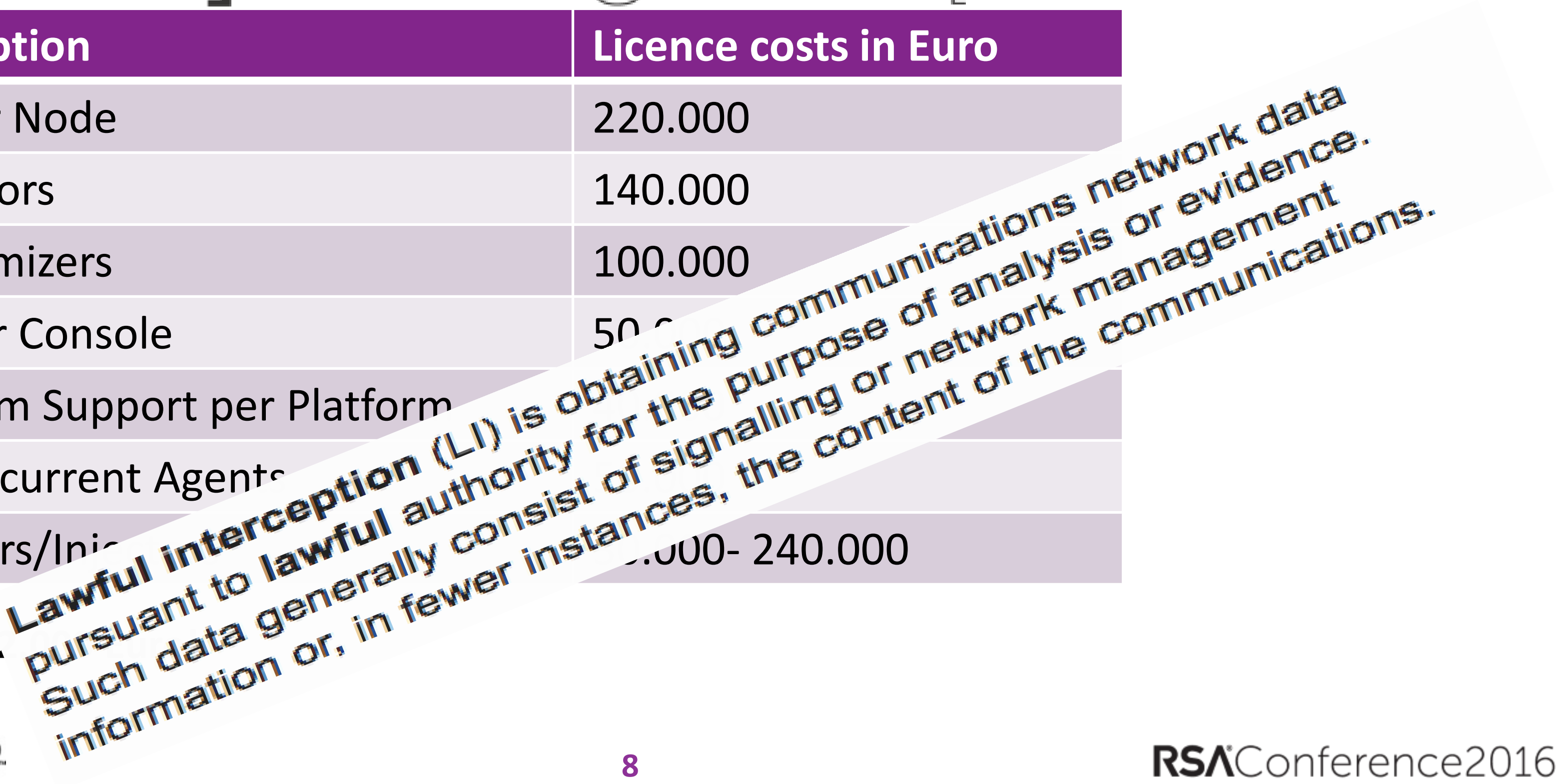
Description	Product Code	Yearly License Fees in € EUR
Exploit Delivery Service – 1 Year Subscription License for one (1) year subscription to Exploit Delivery Service (EDS). EDS grants you access to a selection of 0-day exploits targeting different applications. The Exploit Delivery Service includes the following key features: - RiTE (RiTE is a Testing Ecosystem) performing validity and security checks daily. - Exploit Delivery Network (EDN) managed by HT and hosted on anonymous systems, providing a secure environment for serving exploits - Requests performed via secured online ticketing. As an example, a request can consist of customer-provided application content (e.g., Word file) and specific infection vector - Delivery of weaponized customer's content (e.g., Word file with embedded exploit), to be sent to the Target by the customer via customer's Tactical Network Injector or other means - Automatic delivery of multi-stage exploits' components - Automatic deletion of all the stages and content from the EDN as soon as the infection is complete **Note:** exploits availability and service process can change without notice.	RCS-EDS	120.000,00
Custom RiTE Scenario – 1 Year subscription One (1) Custom RiTE Scenario subscription for 1 year. RiTE (RiTE is a Testing Environment) is HT target simulation testing system. RiTE runs more than 500 tests every day to evaluate the security and efficacy of the solution components and functionalities. The Custom RiTE Scenario subscription allows you to define your own custom scenario to be run daily in RiTE for 1 Year, for example to test security software that are local to specific countries or communities (e.g., 360.cn in Asian Chinese communities). **Prerequisite**: the scenario is subject to validation from HT Quality Assurance department.	RCS-RTE	20.000,00
Anonymizers Management Services– 1 Year subscription This service includes the complete management of the Anonymizers such as: One (1) Custom RiTE Scenario subscription for 1 year. - System administration - Periodical system health checks - Troubleshooting & support - Administrative costs (e.g., accounting, payment)	RCS-AMS	10.000,00

Tools for lawful interception

Pricelist:]HackingTeam[

Description	Licence costs in Euro
Master Node	220.000
Collectors	140.000
Anonymizers	100.000
10 user Console	50.
Platform Support per Platform	
10 Concurrent Agents	
Infectors/Inj	.000- 240.000

At least **43.**



Lawful interception (LI) is obtaining communications network data pursuant to **lawful** authority for the purpose of analysis or evidence. Such data generally consist of signalling or network management information or, in fewer instances, the content of the communications.

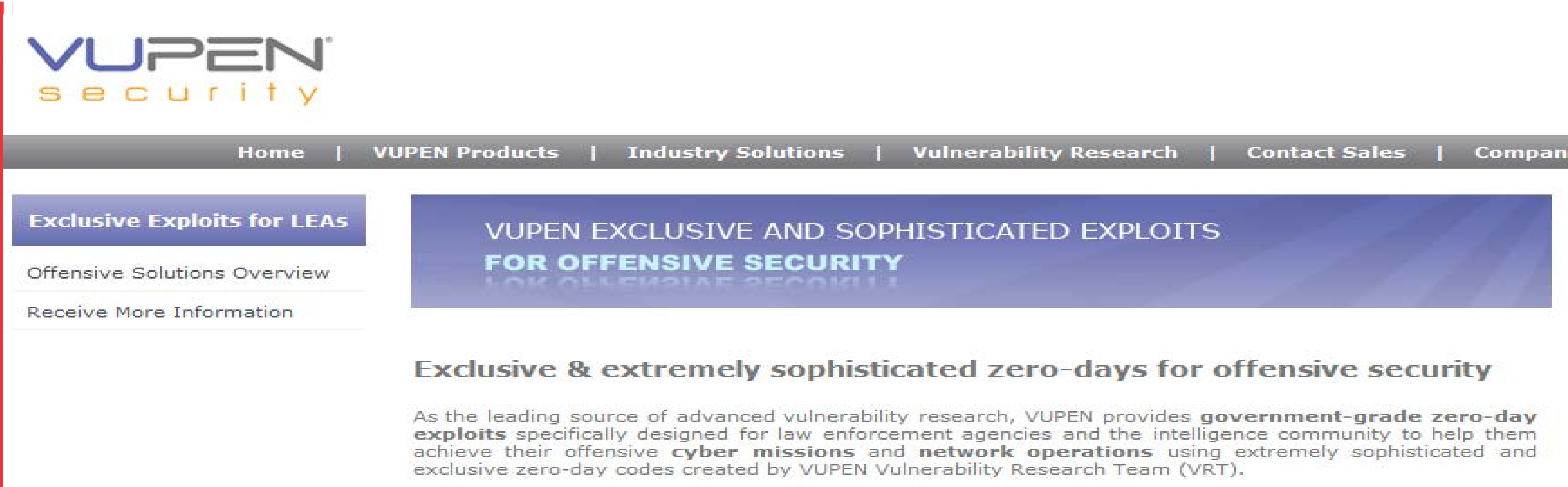
Underground tools price for comparison

Price list:

Description	Licence costs in €/Month	One time fee in €
Malware Checking	27	45
File Dropper and Cryptor	63	186
Botnet framework	36	113
Exploit kit	34	108
Bulletproof Hosting	52	

452 Euro one time fee and monthly costs of 212 Euro

Other players – Vupen Security


VUPEN security
Home | VUPEN Products | Industry Solutions | Vulnerability Research | Contact Sales | Compan
Exclusive Exploits for LEAs
Offensive Solutions Overview
Receive More Information

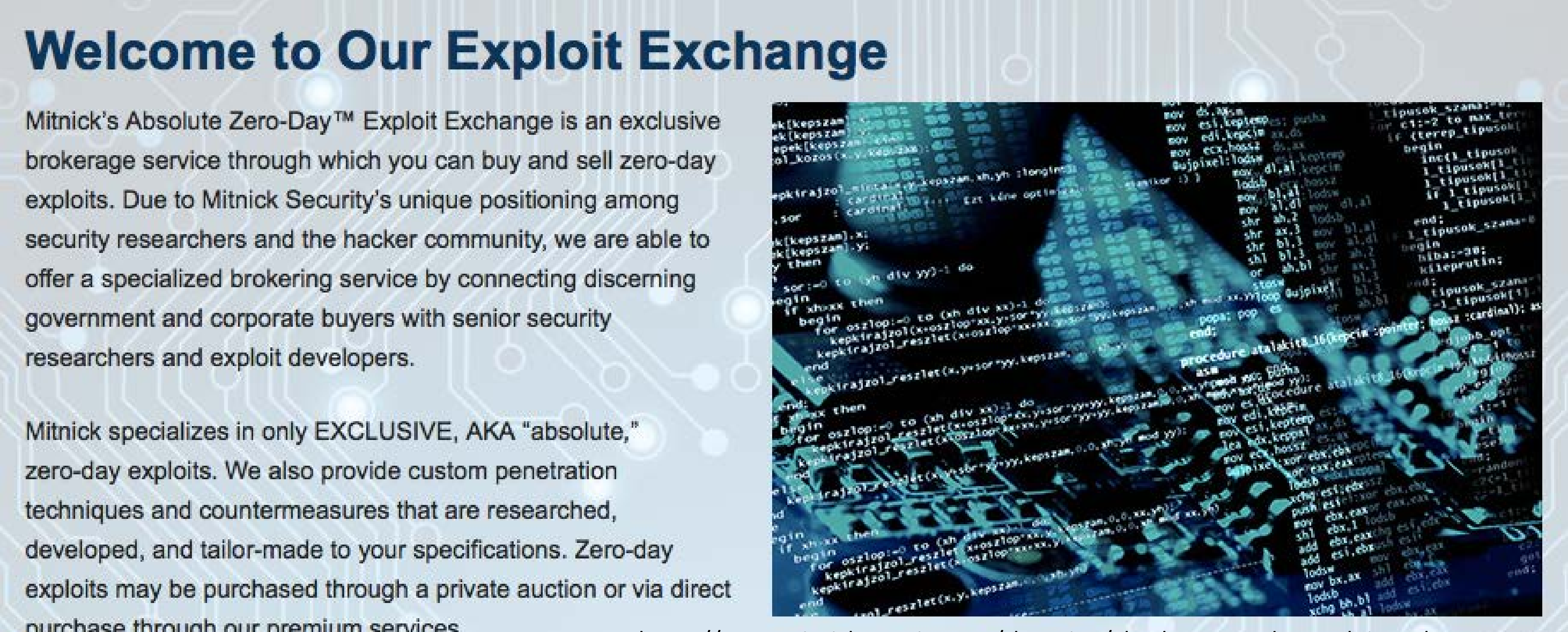
VUPEN EXCLUSIVE AND SOPHISTICATED EXPLOITS
FOR OFFENSIVE SECURITY

Exclusive & extremely sophisticated zero-days for offensive security

As the leading source of advanced vulnerability research, VUPEN provides **government-grade zero-day exploits** specifically designed for law enforcement agencies and the intelligence community to help them achieve their offensive **cyber missions** and **network operations** using extremely sophisticated and exclusive zero-day codes created by VUPEN Vulnerability Research Team (VRT).

Source: http://www.vupen.com/english/services/lea-index.php

Other players – MitnickSecurity.com



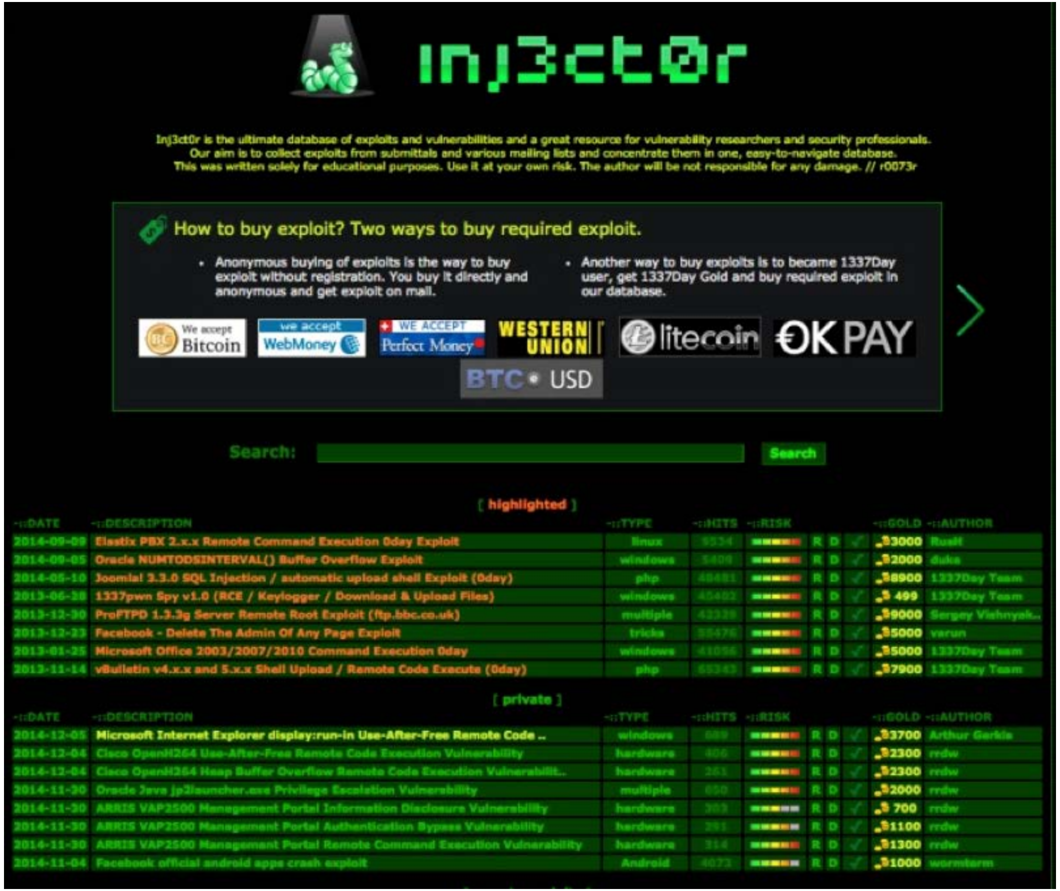
Welcome to Our Exploit Exchange

Mitnick's Absolute Zero-Day™ Exploit Exchange is an exclusive brokerage service through which you can buy and sell zero-day exploits. Due to Mitnick Security's unique positioning among security researchers and the hacker community, we are able to offer a specialized brokering service by connecting discerning government and corporate buyers with senior security researchers and exploit developers.

Mitnick specializes in only EXCLUSIVE, AKA "absolute," zero-day exploits. We also provide custom penetration techniques and countermeasures that are researched, developed, and tailor-made to your specifications. Zero-day exploits may be purchased through a private auction or via direct purchase through our premium services.

Source: https://www.mitnicksecurity.com/shopping/absolute-zero-day-exploit-exchange

Underground Forums



Inj3ct0r is the ultimate database of exploits and vulnerabilities and a great resource for vulnerability researchers and security professionals.
Our aim is to collect exploits from submittals and various mailing lists and concentrate them in one, easy-to-navigate database.
This was written solely for educational purposes. Use it at your own risk. The author will be not responsible for any damage. // r0073r

How to buy exploit? Two ways to buy required exploit.

- Anonymous buying of exploits is the way to buy exploit without registration. You buy it directly and anonymous and get exploit on mail.
- Another way to buy exploits is to became 1337Day user, get 1337Day Gold and buy required exploit in our database.

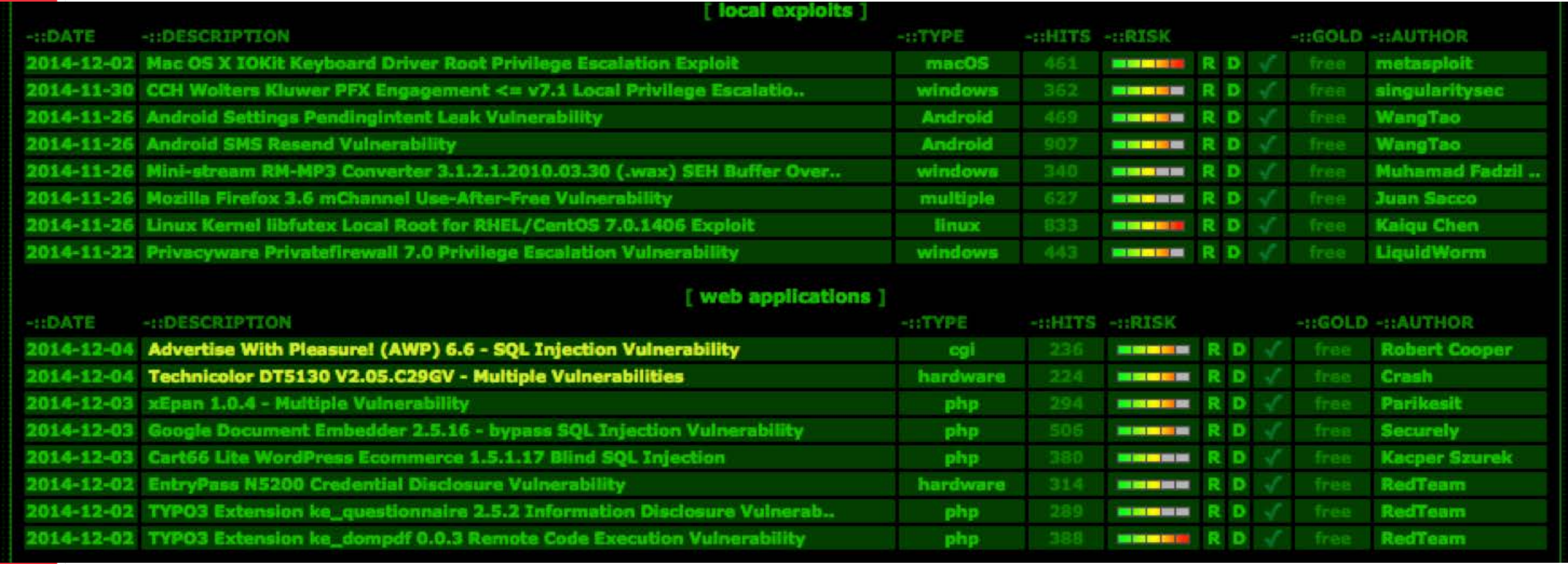
[highlighted]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK				-::GOLD	-::AUTHOR
2014-09-09	Elastix PBX 2.x.x Remote Command Execution 0day Exploit	linux	9534	■■■■■■■	R	D	✓	3000	Rusit
2014-09-05	Oracle NUMTODSINTERVAL() Buffer Overflow Exploit	windows	5409	■■■■■■■	R	D	✓	2000	duke
2014-05-10	Joomla! 3.3.0 SQL Injection / automatic upload shell Exploit (0day)	php	48481	■■■■■■■	R	D	✓	8900	1337Day Team
2013-06-20	1337pwn Spy v1.0 (RCE / Keylogger / Download & Upload Files)	windows	45402	■■■■■■■	R	D	✓	499	1337Day Team
2013-12-30	ProFTPD 1.3.3g Server Remote Root Exploit (ftp.bbc.co.uk)	multiple	42328	■■■■■■■	R	D	✓	9000	Sergey Vishnyak..
2013-12-23	Facebook - Delete The Admin Of Any Page Exploit	tricks	55476	■■■■■■■	R	D	✓	5000	varun
2013-01-25	Microsoft Office 2003/2007/2010 Command Execution 0day	windows	41056	■■■■■■■	R	D	✓	5000	1337Day Team
2013-11-14	vBulletin v4.x.x and 5.x.x Shell Upload / Remote Code Execute (0day)	php	65343	■■■■■■■	R	D	✓	7900	1337Day Team

[private]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK				-::GOLD	-::AUTHOR
2014-12-05	Microsoft Internet Explorer display:run-in Use-After-Free Remote Code ..	windows	689	■■■■■■■	R	D	✓	3700	Arthur Gerkis
2014-12-04	Cisco OpenH264 Use-After-Free Remote Code Execution Vulnerability	hardware	406	■■■■■■■	R	D	✓	2300	rrdw
2014-12-04	Cisco OpenH264 Heap Buffer Overflow Remote Code Execution Vulnerabilit..	hardware	261	■■■■■■■	R	D	✓	2300	rrdw
2014-11-20	Oracle Java jp2launcher.exe Privilege Escalation Vulnerability	multiple	650	■■■■■■■	R	D	✓	2000	rrdw
2014-11-20	ARRIS VAP2500 Management Portal Information Disclosure Vulnerability	hardware	303	■■■■■□□	R	D	✓	700	rrdw
2014-11-20	ARRIS VAP2500 Management Portal Authentication Bypass Vulnerability	hardware	291	■■■■■■□	R	D	✓	1100	rrdw
2014-11-20	ARRIS VAP2500 Management Portal Remote Command Execution Vulnerability	hardware	314	■■■■■■■	R	D	✓	1300	rrdw
2014-11-04	Facebook official android apps crash exploit	Android	4073	■■■■■■□	R	D	✓	1000	wormsterm

Underground Forums



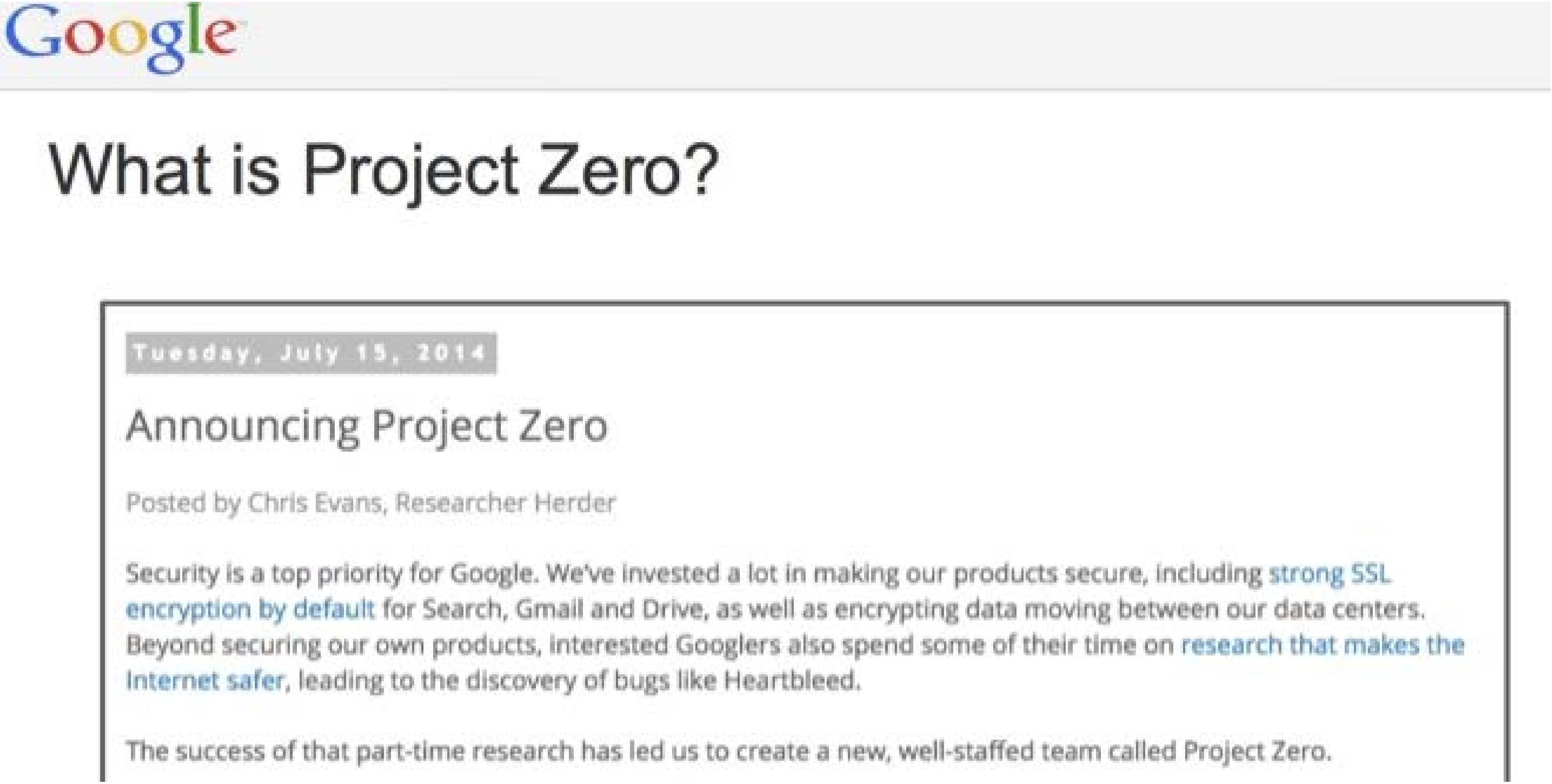
[local exploits]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK				-::GOLD	-::AUTHOR
2014-12-02	Mac OS X IOKit Keyboard Driver Root Privilege Escalation Exploit	macOS	461	🟩🟩🟨🟧🟥	R	D	✓	free	metasploit
2014-11-30	CCH Wolters Kluwer PFX Engagement <= v7.1 Local Privilege Escalatio..	windows	362	🟩🟩🟨🟧⬜	R	D	✓	free	singularitysec
2014-11-26	Android Settings Pendingintent Leak Vulnerability	Android	469	🟩🟩🟨🟧⬜	R	D	✓	free	WangTao
2014-11-26	Android SMS Resend Vulnerability	Android	907	🟩🟩🟨🟧⬜	R	D	✓	free	WangTao
2014-11-26	Mini-stream RM-MP3 Converter 3.1.2.1.2010.03.30 (.wax) SEH Buffer Over..	windows	340	🟩🟩🟨⬜⬜	R	D	✓	free	Muhamad Fadzil ..
2014-11-26	Mozilla Firefox 3.6 mChannel Use-After-Free Vulnerability	multiple	627	🟩🟩🟨⬜⬜	R	D	✓	free	Juan Sacco
2014-11-26	Linux Kernel libfutex Local Root for RHEL/CentOS 7.0.1406 Exploit	linux	833	🟩🟩🟨🟧🟥	R	D	✓	free	Kaiqu Chen
2014-11-22	Privacyware Privatefirewall 7.0 Privilege Escalation Vulnerability	windows	443	🟩🟩🟨🟧⬜	R	D	✓	free	LiquidWorm

[web applications]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK				-::GOLD	-::AUTHOR
2014-12-04	Advertise With Pleasure! (AWP) 6.6 - SQL Injection Vulnerability	cgi	236	🟩🟩🟨🟧⬜	R	D	✓	free	Robert Cooper
2014-12-04	Technicolor DT5130 V2.05.C29GV - Multiple Vulnerabilities	hardware	224	🟩🟩🟨🟧⬜	R	D	✓	free	Crash
2014-12-03	xEpan 1.0.4 - Multiple Vulnerability	php	294	🟩🟩🟨🟧⬜	R	D	✓	free	Parikesit
2014-12-03	Google Document Embedder 2.5.16 - bypass SQL Injection Vulnerability	php	506	🟩🟩🟨🟧⬜	R	D	✓	free	Securely
2014-12-03	Cart66 Lite WordPress Ecommerce 1.5.1.17 Blind SQL Injection	php	380	🟩🟩🟨⬜⬜	R	D	✓	free	Kacper Szurek
2014-12-02	EntryPass N5200 Credential Disclosure Vulnerability	hardware	314	🟩🟩🟨⬜⬜	R	D	✓	free	RedTeam
2014-12-02	TYPO3 Extension ke_questionnaire 2.5.2 Information Disclosure Vulnerab..	php	289	🟩🟩🟨⬜⬜	R	D	✓	free	RedTeam
2014-12-02	TYPO3 Extension ke_dompdf 0.0.3 Remote Code Execution Vulnerability	php	388	🟩🟩🟨🟧🟥	R	D	✓	free	RedTeam

Security Researchers – the good guys!



Google

What is Project Zero?

Tuesday, July 15, 2014

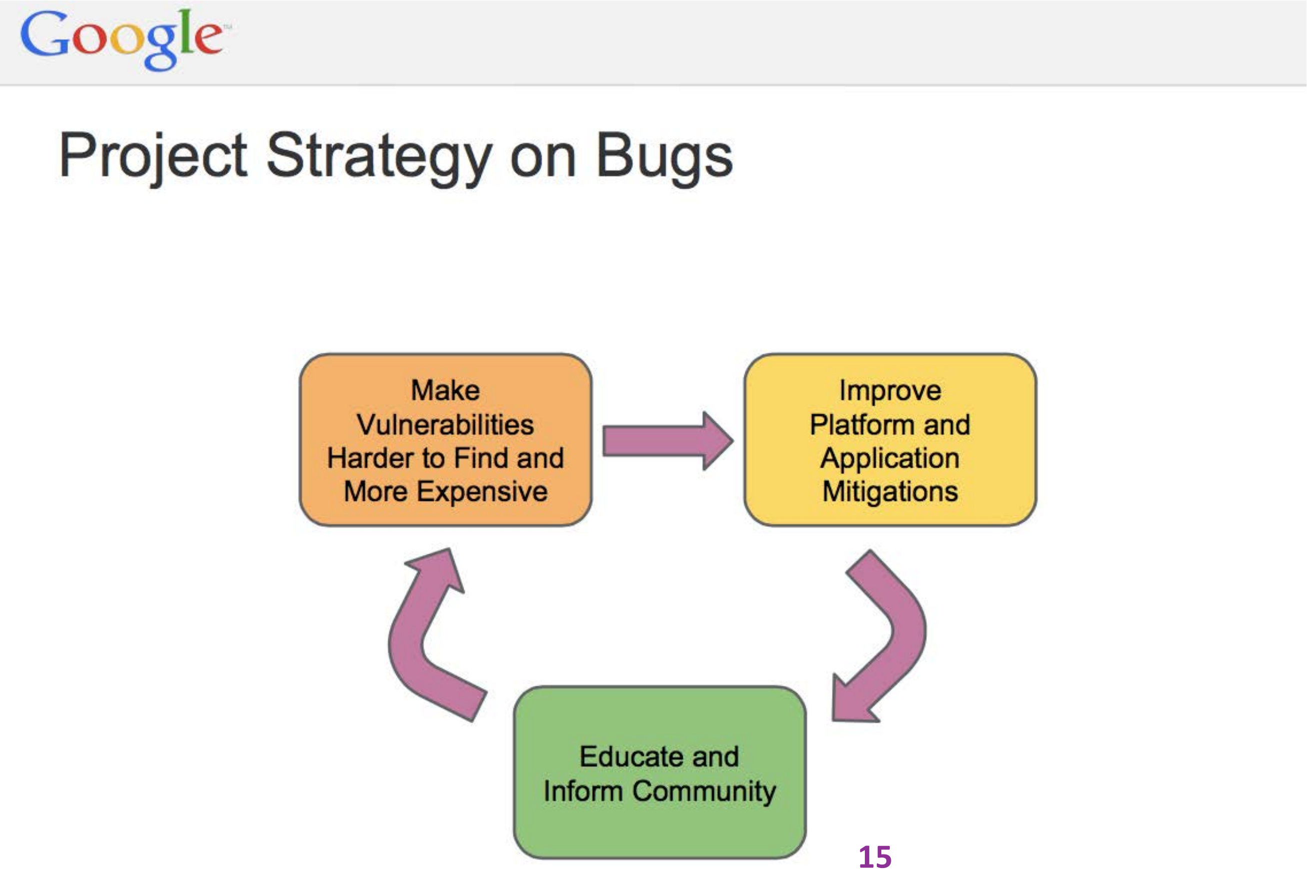
Announcing Project Zero

Posted by Chris Evans, Researcher Herder

Security is a top priority for Google. We've invested a lot in making our products secure, including strong SSL encryption by default for Search, Gmail and Drive, as well as encrypting data moving between our data centers. Beyond securing our own products, interested Googlers also spend some of their time on research that makes the Internet safer, leading to the discovery of bugs like Heartbleed.

The success of that part-time research has led us to create a new, well-staffed team called Project Zero.

Security Researchers – the good guys!



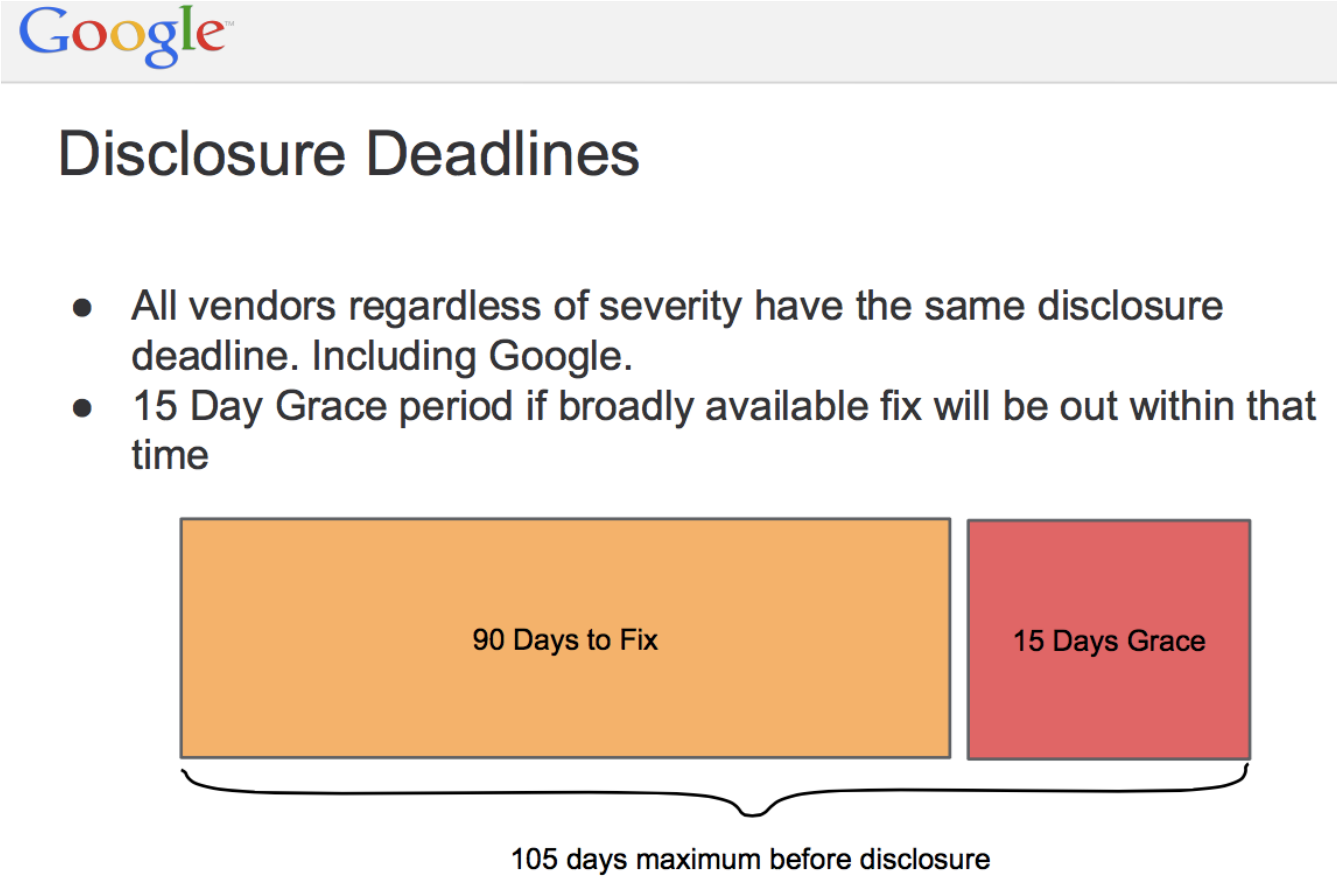
Project Strategy on Bugs

Make Vulnerabilities Harder to Find and More Expensive

Improve Platform and Application Mitigations

Educate and Inform Community

Disclosure deadlines – a hot topic



Google

Disclosure Deadlines

- All vendors regardless of severity have the same disclosure deadline. Including Google.
- 15 Day Grace period if broadly available fix will be out within that time

90 Days to Fix

15 Days Grace

105 days maximum before disclosure

Disclosure deadlines at Trend Micro

Upon discovery of a possible vulnerability Trend Micro will seek to contact the affected vendors through email, social media (privately) or telephone, whichever is applicable. We will inform them about the nature of the vulnerability, our assessment of how critical the vulnerability is, and how soon we would be expecting their reply.

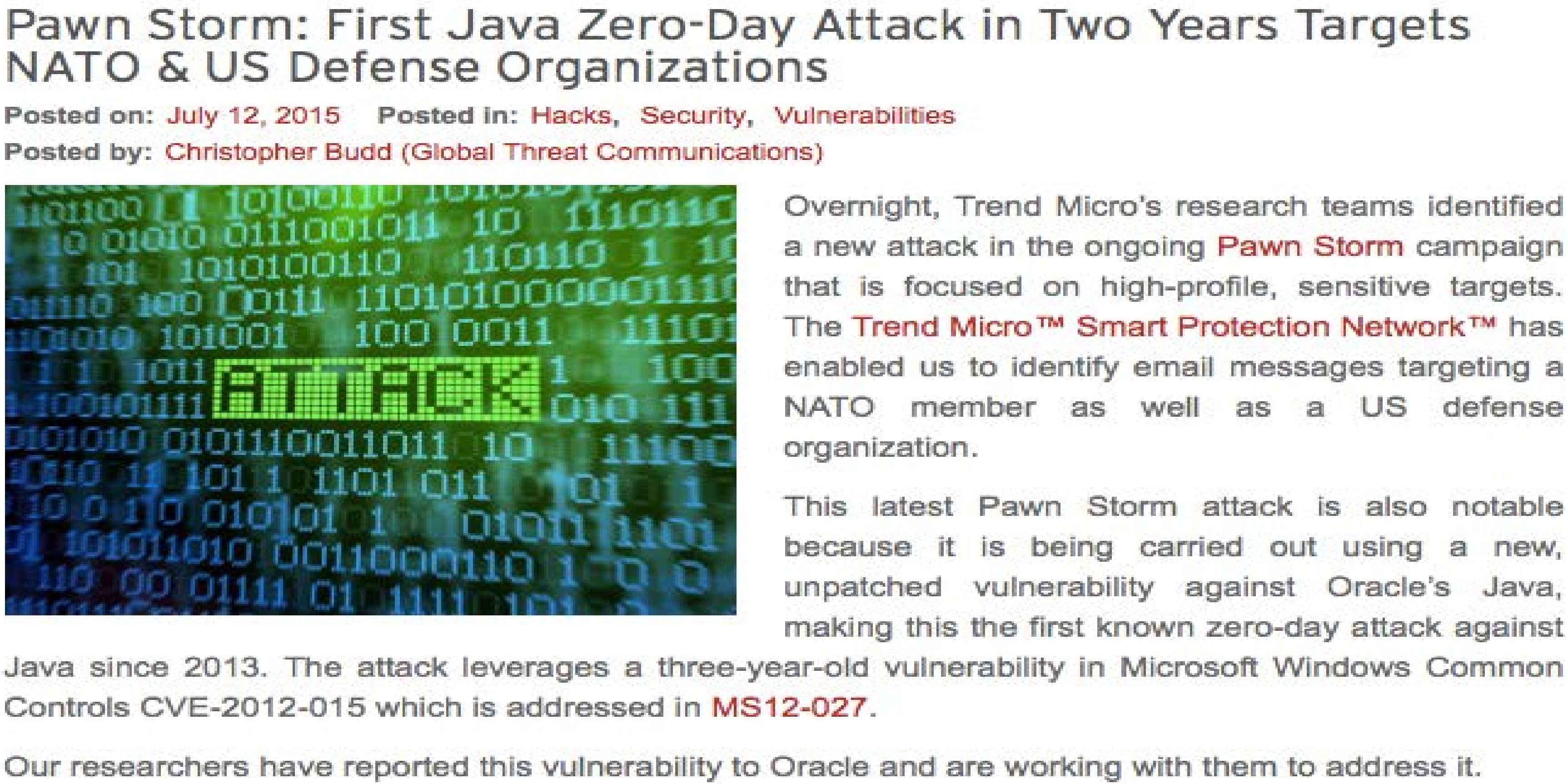
We will then give the affected vendor up to 48 hours to give us a non-automated reply.

If the vendor replies within 48 hours, we will next coordinate with the vendor for an acceptable time frame for a security update. The acceptable time frame lies mostly on the complexity of the vulnerability, but in general, will not exceed 12 weeks from the time of the report.

Disclosure deadlines at Trend Micro

The above guidelines are applicable for most vulnerability findings. The only exceptional treatment of a vulnerability is if a **vulnerability is under active attack by an in-the-wild exploit (i.e. 0-day)**. In this case, in the interest of the safety and security of the general public, Trend Micro will disclose zero-day exploit information within the next 24 hours of vulnerability discovery.
We will, however, make sure to inform the vendor that we are reporting about the vulnerability within the next 24 hours, and any action they will be undertaking to address the issue will be taken into account in the publication including any Trend Micro solutions to protect our customers. We will not be disclosing the full vulnerability information but enough technical details to allow IT admins to determine the appropriate workarounds in the case of unavailability of a timely patch.

One Example – Java Zero Day discovery



Pawn Storm: First Java Zero-Day Attack in Two Years Targets NATO & US Defense Organizations

Posted on: July 12, 2015 **Posted in:** Hacks, Security, Vulnerabilities

Posted by: Christopher Budd (Global Threat Communications)

Overnight, Trend Micro's research teams identified a new attack in the ongoing Pawn Storm campaign that is focused on high-profile, sensitive targets. The Trend Micro™ Smart Protection Network™ has enabled us to identify email messages targeting a NATO member as well as a US defense organization.

This latest Pawn Storm attack is also notable because it is being carried out using a new, unpatched vulnerability against Oracle's Java, making this the first known zero-day attack against Java since 2013. The attack leverages a three-year-old vulnerability in Microsoft Windows Common Controls CVE-2012-015 which is addressed in MS12-027.

Our researchers have reported this vulnerability to Oracle and are working with them to address it.

One Example – Java Zero Day

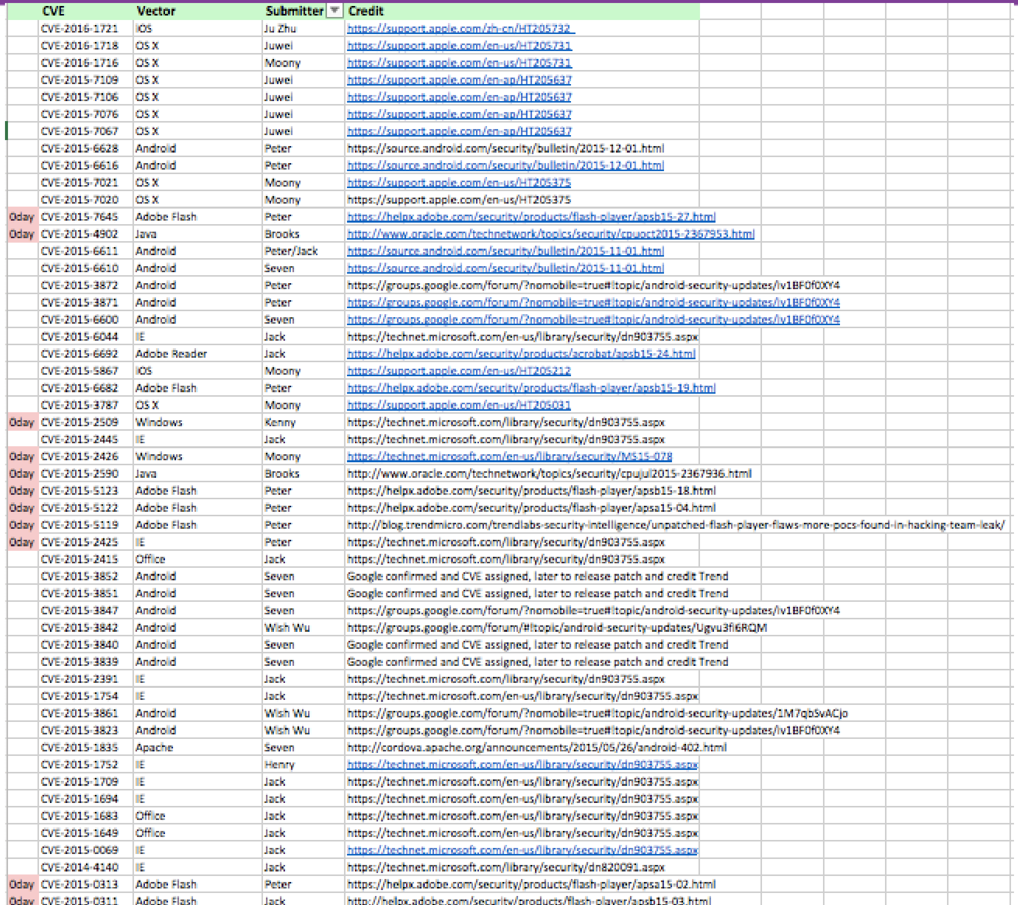
1. July 11 – Vulnerability Research team discovered the Java zero-day, and linked it to Pawn Storm
2. July 14 – Oracle released an advisory and patched the vulnerability
3. July 14 – We published FTR's detailed findings of the APT attack chain

July 15th, our researchers and InfoSec found that the infection URL as discussed in #3 (contained in spear phishing emails and hosting the zero-day exploit) has been modified so that it redirects traffic to http://trendmicro.eu.

InfoSec has confirmed that there is no compromise on our infrastructure, and InfoSec had these notes on why the attackers will redirect traffic to us:

- In retaliation on Trend disclosing their recent campaign
- By pointing to our host it may mislead other system owners to associate our IP 216.104.20.189 to the attack, and may mistakenly block our IP
- Other researchers tracing this campaign may also be misled into thinking our systems are compromised and mis-used by this actors

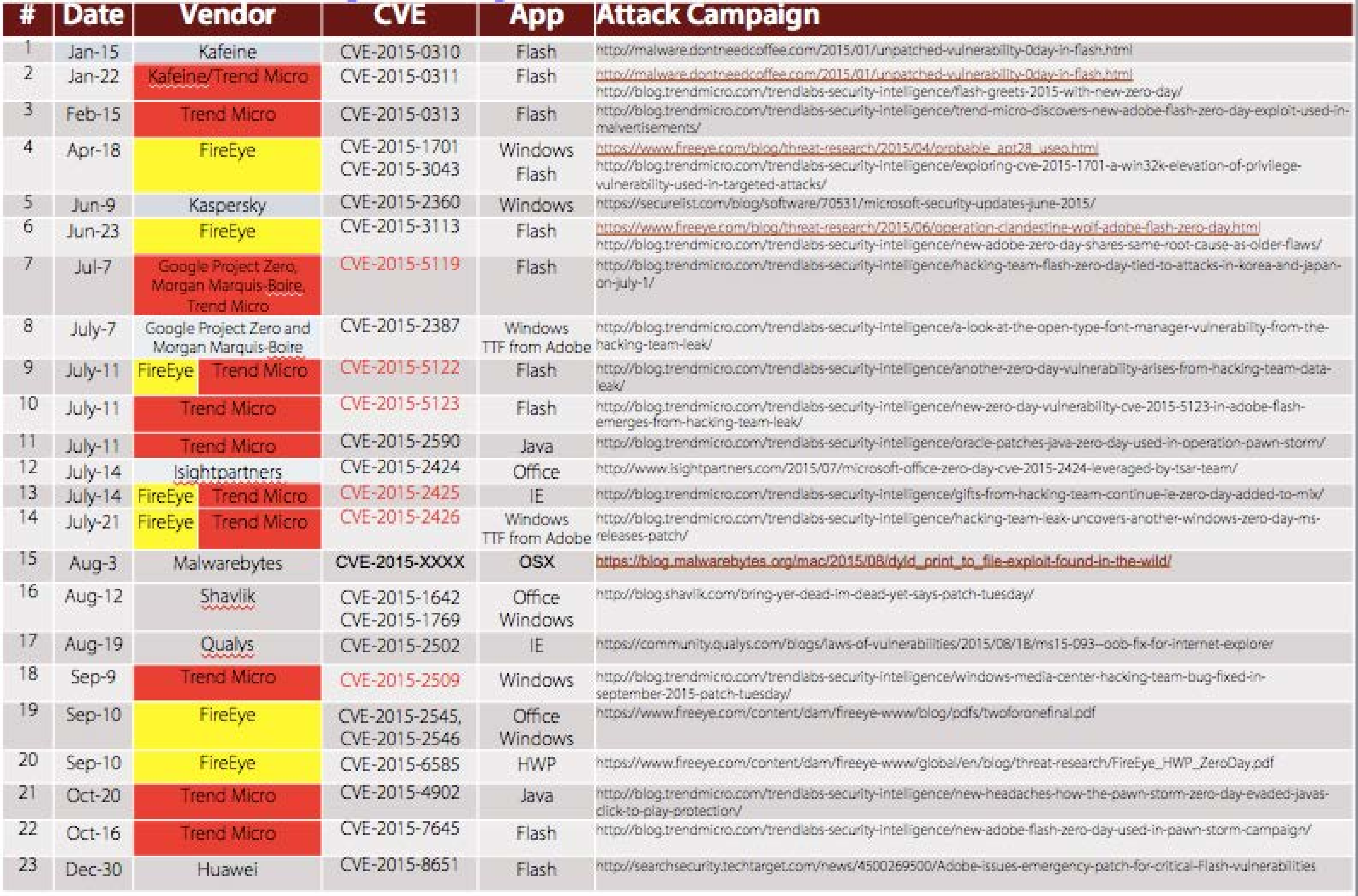
Inside Trend Micro - The small print



	CVE	Vector	Submitter	Credit
	CVE-2016-1721	iOS	Ju Zhu	https://support.apple.com/zh-cn/HT205732
	CVE-2016-1718	OS X	Juwei	https://support.apple.com/en-us/HT205731
	CVE-2016-1716	OS X	Moony	https://support.apple.com/en-us/HT205731
	CVE-2015-7109	OS X	Juwei	https://support.apple.com/en-ap/HT205637
	CVE-2015-7106	OS X	Juwei	https://support.apple.com/en-ap/HT205637
	CVE-2015-7076	OS X	Juwei	https://support.apple.com/en-ap/HT205637
	CVE-2015-7067	OS X	Juwei	https://support.apple.com/en-ap/HT205637
	CVE-2015-6628	Android	Peter	https://source.android.com/security/bulletin/2015-12-01.html
	CVE-2015-6616	Android	Peter	https://source.android.com/security/bulletin/2015-12-01.html
	CVE-2015-7021	OS X	Moony	https://support.apple.com/en-us/HT205375
	CVE-2015-7020	OS X	Moony	https://support.apple.com/en-us/HT205375
0day	CVE-2015-7645	Adobe Flash	Peter	https://helpx.adobe.com/security/products/flash-player/apsb15-27.html
0day	CVE-2015-4902	Java	Brooks	http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
	CVE-2015-6611	Android	Peter/Jack	https://source.android.com/security/bulletin/2015-11-01.html
	CVE-2015-6610	Android	Seven	https://source.android.com/security/bulletin/2015-11-01.html
	CVE-2015-3872	Android	Peter	https://groups.google.com/forum/?nomobile=true#!topic/android-security-updates/Iv1BF0f0XY4
	CVE-2015-3871	Android	Peter	https://groups.google.com/forum/?nomobile=true#!topic/android-security-updates/Iv1BF0f0XY4
	CVE-2015-6600	Android	Seven	https://groups.google.com/forum/?nomobile=true#!topic/android-security-updates/Iv1BF0f0XY4
	CVE-2015-6044	IE	Jack	https://technet.microsoft.com/en-us/library/security/dn903755.aspx
	CVE-2015-6692	Adobe Reader	Jack	https://helpx.adobe.com/security/products/acrobat/apsb15-24.html
	CVE-2015-5867	iOS	Moony	https://support.apple.com/en-us/HT205212
	CVE-2015-6682	Adobe Flash	Peter	https://helpx.adobe.com/security/products/flash-player/apsb15-19.html
	CVE-2015-3787	OS X	Moony	https://support.apple.com/en-us/HT205031
0day	CVE-2015-2509	Windows	Kenny	https://technet.microsoft.com/library/security/dn903755.aspx
	CVE-2015-2445	IE	Jack	https://technet.microsoft.com/library/security/dn903755.aspx
0day	CVE-2015-2426	Windows	Moony	https://technet.microsoft.com/en-us/library/security/MS15-078
0day	CVE-2015-2590	Java	Brooks	http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
0day	CVE-2015-5123	Adobe Flash	Peter	https://helpx.adobe.com/security/products/flash-player/apsb15-18.html
0day	CVE-2015-5122	Adobe Flash	Peter	https://helpx.adobe.com/security/products/flash-player/apsa15-04.html
0day	CVE-2015-5119	Adobe Flash	Peter	http://blog.trendmicro.com/trendlabs-security-intelligence/unpatched-flash-player-flaws-more-pocs-found-in-hacking-team-leak/
0day	CVE-2015-2425	IE	Peter	https://technet.microsoft.com/library/security/dn903755.aspx
	CVE-2015-2415	Office	Jack	https://technet.microsoft.com/library/security/dn903755.aspx
	CVE-2015-3852	Android	Seven	Google confirmed and CVE assigned, later to release patch and credit Trend
	CVE-2015-3851	Android	Seven	Google confirmed and CVE assigned, later to release patch and credit Trend
	CVE-2015-3847	Android	Seven	https://groups.google.com/forum/?nomobile=true#!topic/android-security-updates/Iv1BF0f0XY4
	CVE-2015-3842	Android	Wish Wu	https://groups.google.com/forum/#!topic/android-security-updates/Ugvu3fi6RQM
	CVE-2015-3840	Android	Seven	Google confirmed and CVE assigned, later to release patch and credit Trend
	CVE-2015-3839	Android	Seven	Google confirmed and CVE assigned, later to release patch and credit Trend
	CVE-2015-2391	IE	Jack	https://technet.microsoft.com/library/security/dn903755.aspx
	CVE-2015-1754	IE	Jack	https://technet.microsoft.com/en-us/library/security/dn903755.aspx
	CVE-2015-3861	Android	Wish Wu	https://groups.google.com/forum/?nomobile=true#!topic/android-security-updates/1M7qbSvACjo
	CVE-2015-3823	Android	Wish Wu	https://groups.google.com/forum/?nomobile=true#!topic/android-security-updates/Iv1BF0f0XY4
	CVE-2015-1835	Apache	Seven	http://cordova.apache.org/announcements/2015/05/26/android-402.html
	CVE-2015-1752	IE	Henry	https://technet.microsoft.com/en-us/library/security/dn903755.aspx
	CVE-2015-1709	IE	Jack	https://technet.microsoft.com/en-us/library/security/dn903755.aspx
	CVE-2015-1694	IE	Jack	https://technet.microsoft.com/en-us/library/security/dn903755.aspx
	CVE-2015-1683	Office	Jack	https://technet.microsoft.com/en-us/library/security/dn903755.aspx
	CVE-2015-1649	Office	Jack	https://technet.microsoft.com/en-us/library/security/dn903755.aspx
	CVE-2015-0069	IE	Jack	https://technet.microsoft.com/en-us/library/security/dn903755.aspx
	CVE-2014-4140	IE	Jack	https://technet.microsoft.com/library/security/dn820091.aspx
0day	CVE-2015-0313	Adobe Flash	Peter	https://helpx.adobe.com/security/products/flash-player/apsa15-02.html
0day	CVE-2015-0311	Adobe Flash	Jack	http://helpx.adobe.com/security/products/flash-player/apsb15-03.html

11 vulnerabilities detected by Trend Micro researchers in 2015 turned out to be Zero Day Threats!

A bit bigger and fairer



#	Date	Vendor	CVE	App	Attack Campaign
1	Jan-15	Kafeine	CVE-2015-0310	Flash	http://malware.dontneedcoffee.com/2015/01/unpatched-vulnerability-0day-in-flash.html
2	Jan-22	Kafeine/Trend Micro	CVE-2015-0311	Flash	http://malware.dontneedcoffee.com/2015/01/unpatched-vulnerability-0day-in-flash.html http://blog.trendmicro.com/trendlabs-security-intelligence/flash-greets-2015-with-new-zero-day/
3	Feb-15	Trend Micro	CVE-2015-0313	Flash	http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-new-adobe-flash-zero-day-exploit-used-in-malvertisements/
4	Apr-18	FireEye	CVE-2015-1701 CVE-2015-3043	Windows Flash	https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html http://blog.trendmicro.com/trendlabs-security-intelligence/exploring-cve-2015-1701-a-win32k-elevation-of-privilege-vulnerability-used-in-targeted-attacks/
5	Jun-9	Kaspersky	CVE-2015-2360	Windows	https://securelist.com/blog/software/70531/microsoft-security-updates-june-2015/
6	Jun-23	FireEye	CVE-2015-3113	Flash	https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-zero-day-shares-same-root-cause-as-older-flaws/
7	Jul-7	Google Project Zero, Morgan Marquis-Boire, Trend Micro	CVE-2015-5119	Flash	http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-zero-day-tied-to-attacks-in-korea-and-japan-on-july-1/
8	July-7	Google Project Zero and Morgan Marquis-Boire	CVE-2015-2387	Windows TTF from Adobe	http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-at-the-open-type-font-manager-vulnerability-from-the-hacking-team-leak/
9	July-11	FireEye Trend Micro	CVE-2015-5122	Flash	http://blog.trendmicro.com/trendlabs-security-intelligence/another-zero-day-vulnerability-arises-from-hacking-team-data-leak/
10	July-11	Trend Micro	CVE-2015-5123	Flash	http://blog.trendmicro.com/trendlabs-security-intelligence/new-zero-day-vulnerability-cve-2015-5123-in-adobe-flash-emerges-from-hacking-team-leak/
11	July-11	Trend Micro	CVE-2015-2590	Java	http://blog.trendmicro.com/trendlabs-security-intelligence/oracle-patches-java-zero-day-used-in-operation-pawn-storm/
12	July-14	Isightpartners	CVE-2015-2424	Office	http://www.isightpartners.com/2015/07/microsoft-office-zero-day-cve-2015-2424-leveraged-by-tsar-team/
13	July-14	FireEye Trend Micro	CVE-2015-2425	IE	http://blog.trendmicro.com/trendlabs-security-intelligence/gifts-from-hacking-team-continue-ie-zero-day-added-to-mix/
14	July-21	FireEye Trend Micro	CVE-2015-2426	Windows TTF from Adobe	http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-leak-uncovers-another-windows-zero-day-ms-releases-patch/
15	Aug-3	Malwarebytes	CVE-2015-XXXX	OSX	https://blog.malwarebytes.org/mac/2015/08/dyld_print_to_file-exploit-found-in-the-wild/
16	Aug-12	Shavlik	CVE-2015-1642 CVE-2015-1769	Office Windows	http://blog.shavlik.com/bring-yer-dead-im-dead-yet-says-patch-tuesday/
17	Aug-19	Qualys	CVE-2015-2502	IE	https://community.qualys.com/blogs/laws-of-vulnerabilities/2015/08/18/ms15-093--oob-fix-for-internet-explorer
18	Sep-9	Trend Micro	CVE-2015-2509	Windows	http://blog.trendmicro.com/trendlabs-security-intelligence/windows-media-center-hacking-team-bug-fixed-in-september-2015-patch-tuesday/
19	Sep-10	FireEye	CVE-2015-2545, CVE-2015-2546	Office Windows	https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/twoforonefinal.pdf
20	Sep-10	FireEye	CVE-2015-6585	HWP	https://www.fireeye.com/content/dam/fireeye-www/global/en/blog/threat-research/FireEye_HWP_ZeroDay.pdf
21	Oct-20	Trend Micro	CVE-2015-4902	Java	http://blog.trendmicro.com/trendlabs-security-intelligence/new-headaches-how-the-pawn-storm-zero-day-evaded-javas-click-to-play-protection/
22	Oct-16	Trend Micro	CVE-2015-7645	Flash	http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/
23	Dec-30	Huawei	CVE-2015-8651	Flash	http://searchsecurity.techtarget.com/news/4500269500/Adobe-issues-emergency-patch-for-critical-Flash-vulnerabilities

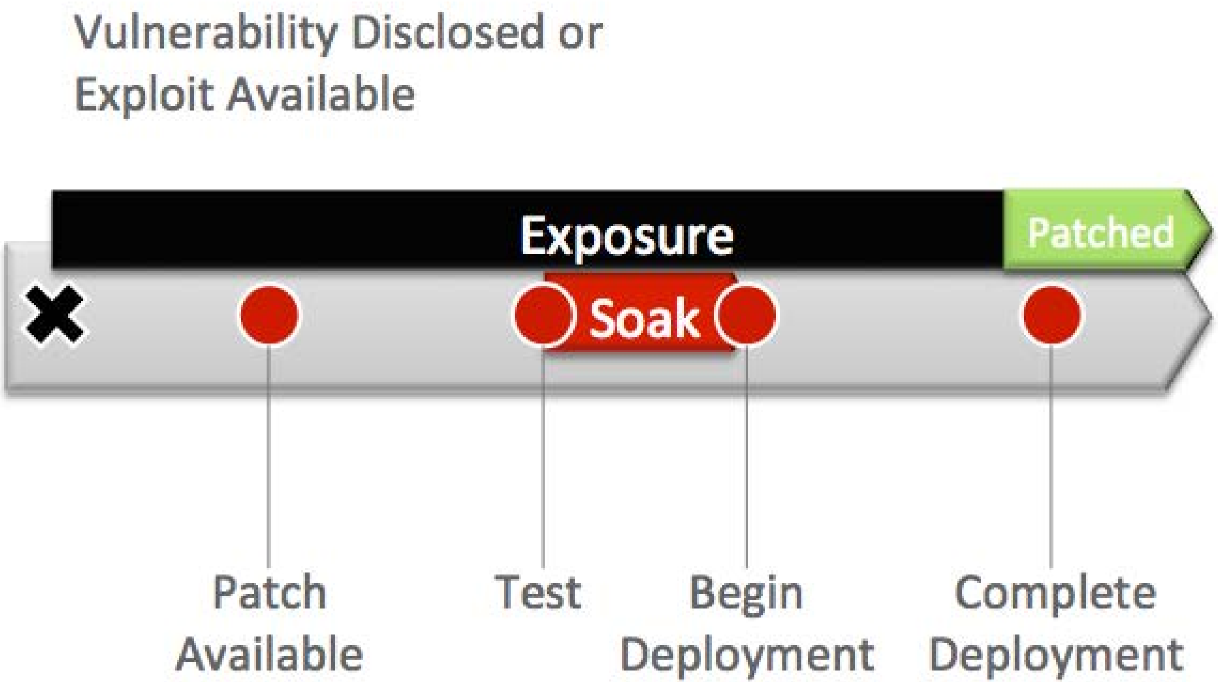
Don’t we hear this all the time?

“How do I ensure our servers are protected against the latest vulnerabilities? ”

Timely Patch Management

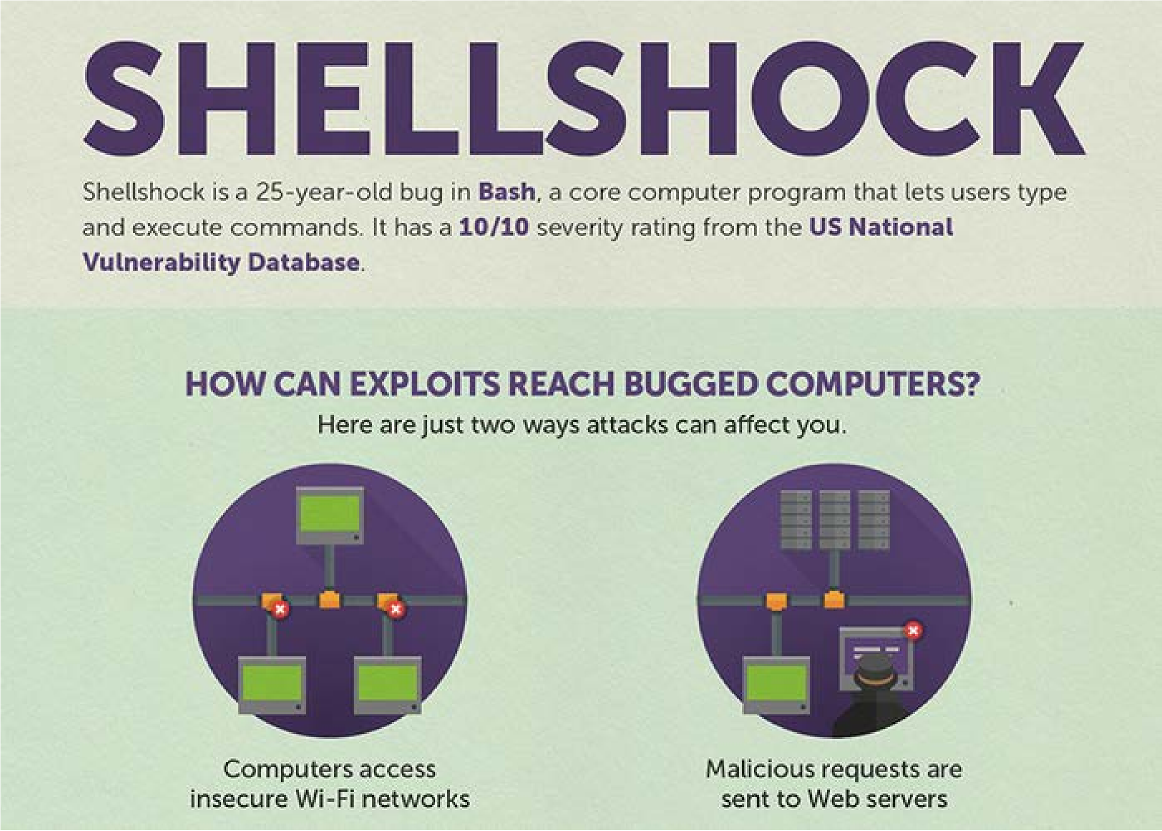
Wishful thinking for a lot of companies!

Reality


Vulnerability Disclosed or Exploit Available
Exposure
Patched
Soak
Patch Available
Test
Begin Deployment
Complete Deployment

Remember Shellshock?

September 2014



SHELLSHOCK

Shellshock is a 25-year-old bug in **Bash**, a core computer program that lets users type and execute commands. It has a **10/10** severity rating from the **US National Vulnerability Database**.

HOW CAN EXPLOITS REACH BUGGED COMPUTERS?

Here are just two ways attacks can affect you.

Computers access insecure Wi-Fi networks

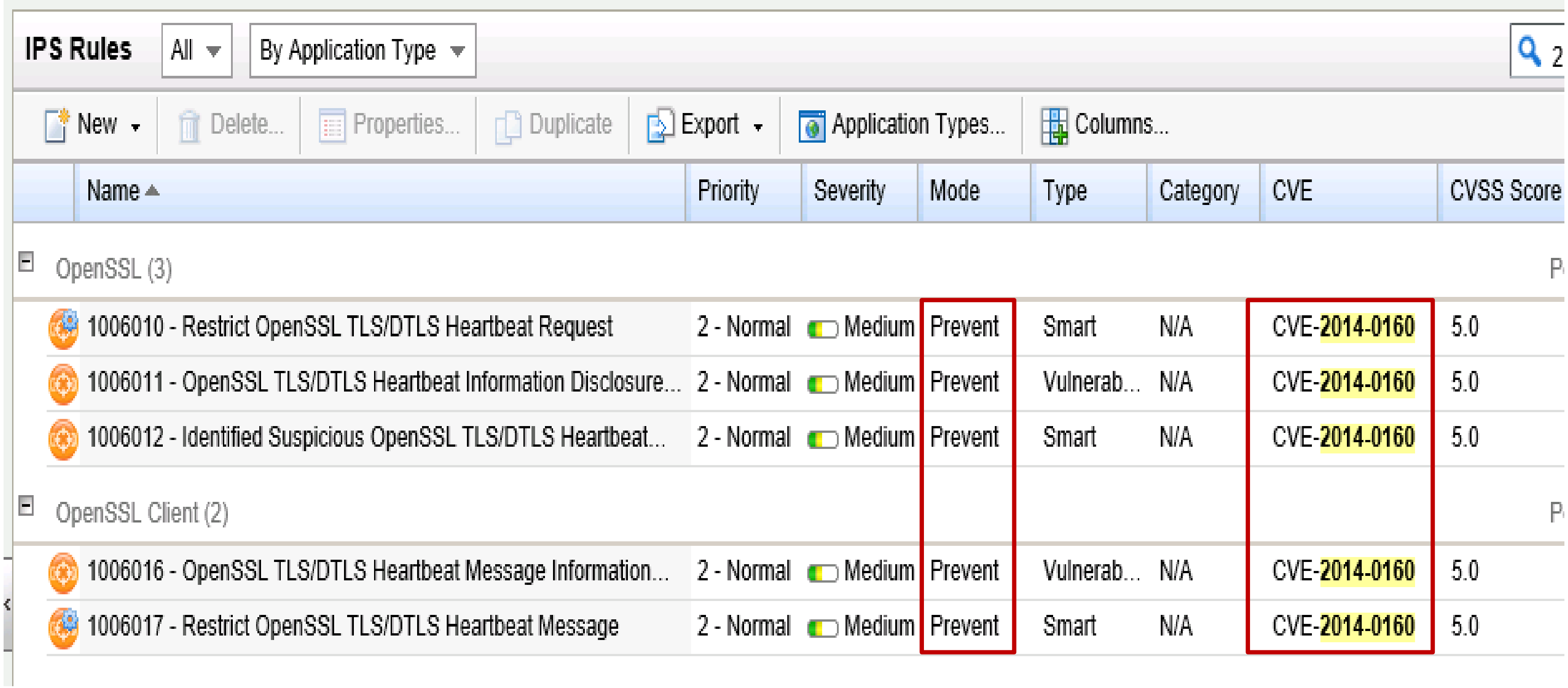
Malicious requests are sent to Web servers

Virtual Patching at work

5 days after ShellShock:
766 attacks blocked!

1 Year later:
70,000+
attacks blocked!

That’s how it looked like with Heartbleed



Name	Priority	Severity	Mode	Type	Category	CVE	CVSS Score
OpenSSL (3)							
1006010 - Restrict OpenSSL TLS/DTLS Heartbeat Request	2 - Normal	Medium	Prevent	Smart	N/A	CVE-2014-0160	5.0
1006011 - OpenSSL TLS/DTLS Heartbeat Information Disclosure...	2 - Normal	Medium	Prevent	Vulnerab...	N/A	CVE-2014-0160	5.0
1006012 - Identified Suspicious OpenSSL TLS/DTLS Heartbeat...	2 - Normal	Medium	Prevent	Smart	N/A	CVE-2014-0160	5.0
OpenSSL Client (2)							
1006016 - OpenSSL TLS/DTLS Heartbeat Message Information...	2 - Normal	Medium	Prevent	Vulnerab...	N/A	CVE-2014-0160	5.0
1006017 - Restrict OpenSSL TLS/DTLS Heartbeat Message	2 - Normal	Medium	Prevent	Smart	N/A	CVE-2014-0160	5.0

Trend Micro acquires Tipping Point

ZERO DAY INITIATIVE

Over **650** vulnerabilities published in 2015

DV Labs

Delivers **11** zero-day filters/week

Block early!

#1 external supplier of bugs to MSFT

Average **181 days** of zero-day predisclosed filter coverage for 2015 bulletins

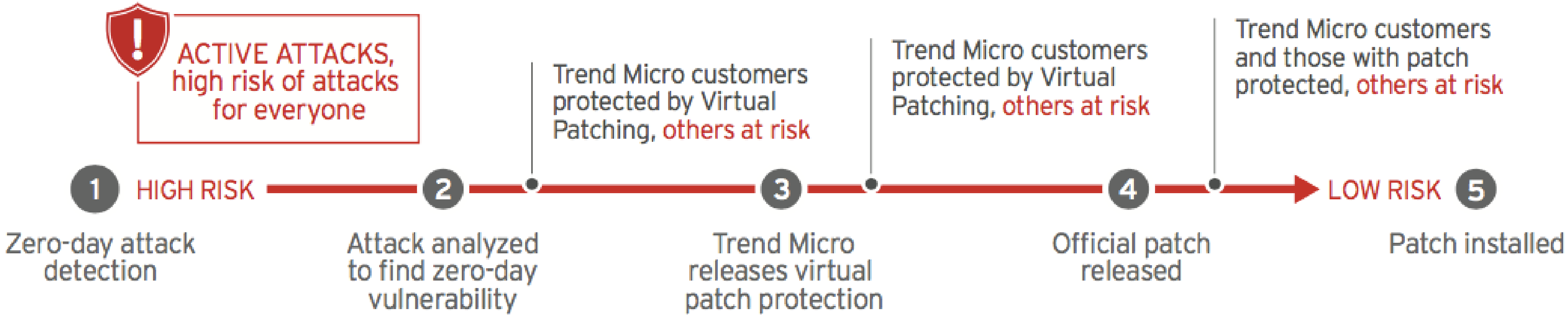
#1 external supplier of Adobe Reader vulnerabilities

Average **101 days** of zero-day predisclosed filter coverage for 2015 bulletins

OpenSSL vulnerability similar to Heartbleed Digital Vaccine provided **43 days** of coverage before OpenSSL Group released a patch

Knowhow buys time!

WITHOUT Trend Micro Vulnerability Research Team



ACTIVE ATTACKS, high risk of attacks for everyone

Trend Micro customers protected by Virtual Patching, others at risk

Trend Micro customers protected by Virtual Patching, others at risk

Trend Micro customers and those with patch protected, others at risk

1 HIGH RISK — Zero-day attack detection

2 — Attack analyzed to find zero-day vulnerability

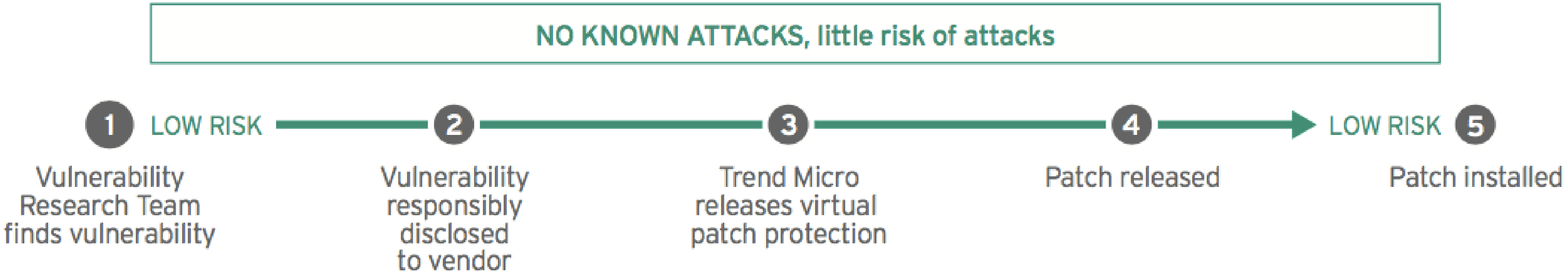
3 — Trend Micro releases virtual patch protection

4 — Official patch released

LOW RISK 5 — Patch installed

Knowhow buys time!

WITH Trend Micro Vulnerability Research Team



NO KNOWN ATTACKS, little risk of attacks

1 LOW RISK — Vulnerability Research Team finds vulnerability

2 — Vulnerability responsibly disclosed to vendor

3 — Trend Micro releases virtual patch protection

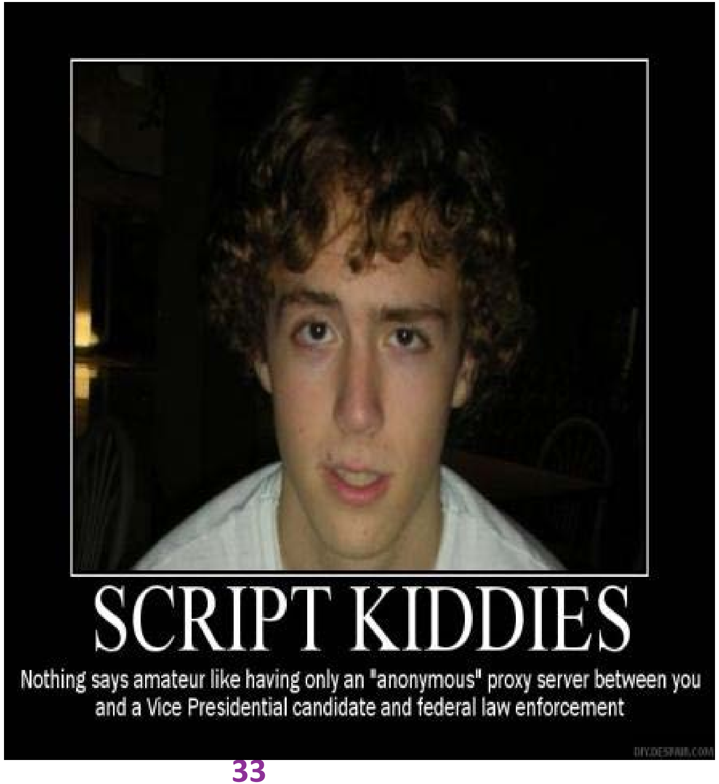
4 — Patch released

LOW RISK 5 — Patch installed

Great for risk assessment!

Rule triggered: Known vulnerability – known for 6 month +

Attacker profile:


SCRIPT KIDDIES
Nothing says amateur like having only an "anonymous" proxy server between you and a Vice Presidential candidate and federal law enforcement
DIY.DESPAIR.COM

Great for risk assessment!

Rule triggered: Known vulnerability – known for less than 6 month

Attacker profile:

Cyber Criminal

Great for risk assessment!

Rule triggered: No CVE assigned, no patch available

Attacker profile:

Nation State,
Elite-Hacker

Apply what you have learned today

Accept that you always will be behind with patching

Don’t use this as an excuse not to do proper patch management!

Buy time to patch with Virtual Patching

Apply this to all your systems – your cloud systems are vulnerable too!

Don’t treat all incidents the same – focus on the important ones

Listen and learn from the attacks; when they use sophisticated weapons, you are a prime target!

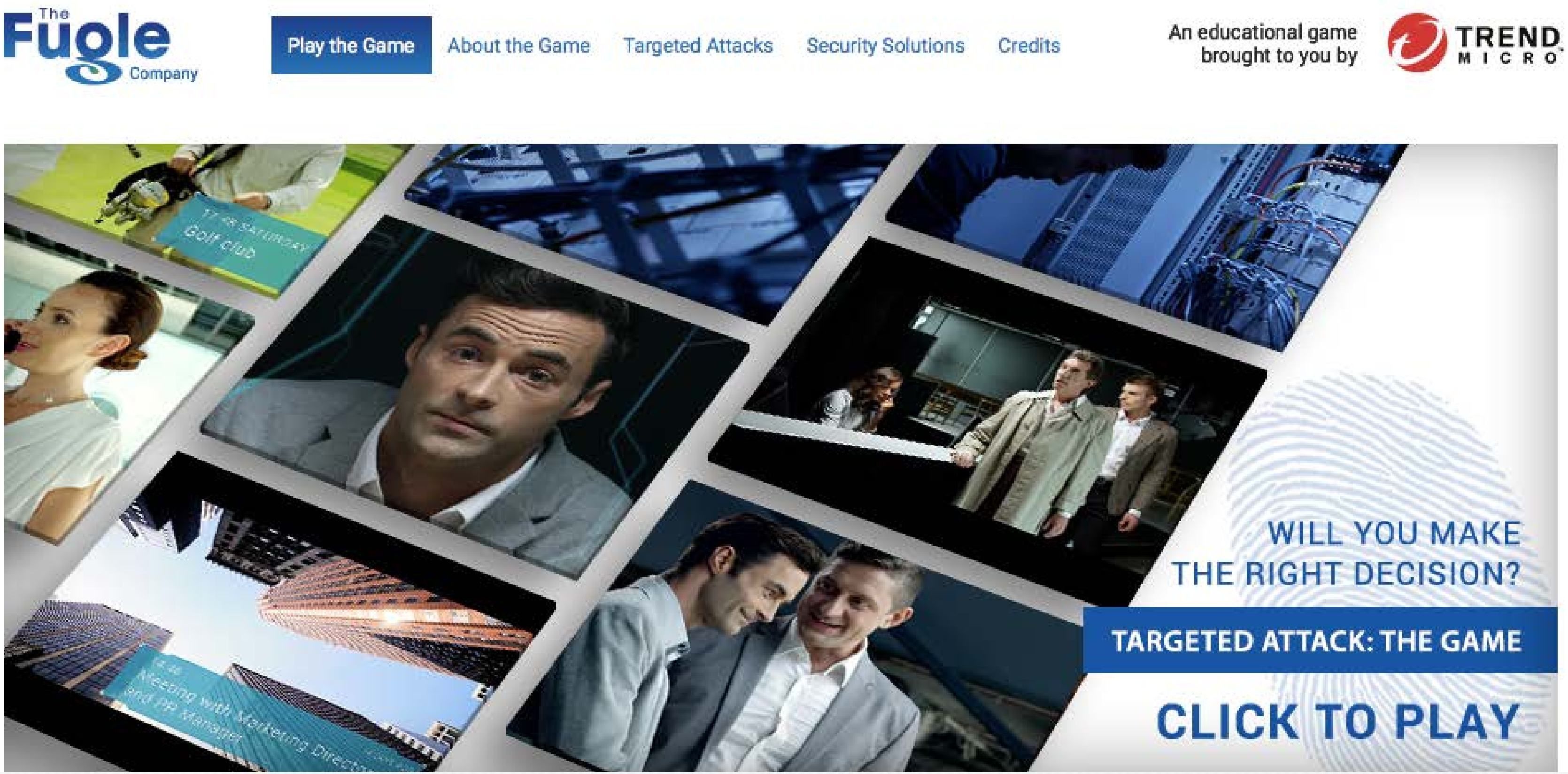
Always remember

A sophisticated attacker is focused and persistent!

“Few if any contemporary computer security controls have prevented a [red team] from easily accessing any information sought.”

Lt Col Roger Schell (USAF) in 1979

targetedattacks.trendmicro.com


The Fugle Company
Play the Game
About the Game
Targeted Attacks
Security Solutions
Credits
An educational game brought to you by
TREND MICRO
Saturday
Golf club
Meeting with Marketing Director and PR Manager
WILL YOU MAKE THE RIGHT DECISION?
TARGETED ATTACK: THE GAME
CLICK TO PLAY

Contact Details

Linkedin: Raimund Genes
Blog: ctoinsights.trendmicro.com
E-Mail: Raimund_Genes@trendmicro.com