Threatpost News Wrap, January 6, 2017

Claudio Guarnieri on Security Without Borders

Costin Raiu on the Importance of…

Threatpost 2016 Year in Review

Threatpost News Wrap, December 16, 2016

Recommended

The Kaspersky Lab Security News Service

Videos

Latest Videos

All

iOS 10 Passcode Bypass Can Access…

BASHLITE Family Of Malware Infects 1…

How to Leak Data From Air-Gapped…

Bruce Schneier on the Integration of…

Chris Valasek Talks Car Hacking, IoT,…

Patrick Wardle on OS X Malware…

Recommended

The Kaspersky Lab Security News Service
The latest Shadowbrokers dump of alleged NSA tools—a cache of Windows exploits—surfaced over the weekend. And for the first time since these unannounced releases started last summer, analysts don’t have the luxury of a free set of files to dig in to.

The group is selling the database for 750 Bitcoin, or close to $608,000 USD, it said in a post to on onlyzero[.]net. From the screenshots made available on the Shadowbrokers Twitter feed, it would appear there is at least one zero-day exploit in the bunch targeting the Windows Server Message Block protocol, a network file-sharing protocol implemented in Windows.
WordPress 4.7.1 Fixes CSRF, XSS, PHPMailer Vulnerabilities

January 12, 2017, 12:38 pm

Second Try at Windows LSASS Patch Addresses Vulnerability

January 11, 2017, 1:01 pm

The ShadowBrokers appeared out of thin air last August, promoting an auction of attacks against enterprise- and telco-grade network gear allegedly belonging to the Equation Group, an APT thought to be associated with the NSA.

Researcher Jacob Williams looked at the screenshots and surmised the zero day by the price the ShadowBrokers are asking.

“Note that most of the tools have apparently been through multiple revisions, adding apparent legitimacy to the claim that these exploits are real,” Williams said. “Though another screenshot hints at a possible zero day SMB exploit, there’s no indication of which exploit names involve SMB (or any other target service).”

Williams also speculated that one of the tools listed called EventLogEdit should be of interest for forensics investigators.

“While we understand that event logs can be cleared and event logging stopped, surgically editing event logs is usually considered to be a very advanced capability (if possible at all). We’ve seen rootkit code over the years (some was published on the now defunct rootkit.com) that supported this feature, but often made the system unstable in the process,” Williams said. “Knowing that some attackers apparently have the ability to edit event logs can be a game changer for an investigation. If Shadow Brokers release this code to the world (as they’ve done previously), it will undermine the reliability of event logs in forensic investigations.”

The screenshots also show a laundry list of plugins labeled DanderSpritz, which Heimdal Security researchers said were listed in some of the documents made public by NSA whistleblower Edward Snowden. The DanderSpritz plugins are available for 250 Bitcoin, while another host of exploits aimed at fuzzing Windows machines is available for 650 Bitcoin. The cache also includes remote access tools, remote code execution exploits for a number of Windows protocols and services such as IIS, RDP and SMB, as well as a SMB backdoor.

In October, the group posted links to downloads of lists of hacked Sun Solaris and Linux servers allegedly compromised by the Equation Group. The servers listed were old, some compromised 15 years ago, and mostly in Iran, Russia, China and Pakistan.

In December, researchers at Flashpoint said an insider with access to an intelligence agency code repository was the likely source of the leak. Their research pointed away from an attack against NSA infrastructure and toward an insider or two.

Researcher Matt Suiche wrote a piece immediately after the first leaks last August speculating that the Shadowbrokers were likely an NSA insider as well. Suiche’s article lists a handful of reasons debunking claims that the files in possession of the Shadowbrokers were mistaken left on a staging server.
The ShadowBrokers today ended their operations, saying they would no longer leak Equation Group exploits.
January 12, 2017, 12:38 pm
Categories: Vulnerabilities, Web Security

**WordPress 4.7.1 Fixes CSRF, XSS, PHPMailer Vulnerabilities**

by Chris Brook

A new WordPress update, pushed this week, resolves eight security issues, including a handful of XSS and CSRF bugs.

Read more...

January 11, 2017, 1:01 pm
Categories: Vulnerabilities

**Second Try at Windows LSASS Patch Addresses Vulnerability**

by Michael Mimoso

Microsoft on Tuesday patched a vulnerability in LSASS, the second attempt it has taken at fixing a remote denial-of-service issue in the critical Windows process.

Read more...

**Top Stories**

**Buggy Domain Validation Forces GoDaddy to Revoke Certs**

January 11, 2017, 4:40 pm

**Two New Edge Exploits Integrated into Sundown Exploit Kit**

January 10, 2017, 11:28 am

**Threatpost News Wrap, January 6, 2017**

January 6, 2017, 12:00 pm

**What Hack? Burlington Electric Speaks Out**
Box.com Plugs Account Data Leakage Flaw

January 3, 2017, 4:28 pm

Threatpost 2016 Year in Review

December 29, 2016, 11:30 am

Congressional Group Says Encryption Backdoors Are a Bad Idea

December 22, 2016, 6:00 am

Stolen Yahoo Data Sold to Spammers, One Government Client

December 19, 2016, 1:42 pm

Microsoft Patches Publicly Disclosed IE, Edge Vulnerabilities

December 13, 2016, 3:27 pm

Alpha Version of Sandboxed Tor Browser Released

December 12, 2016, 1:47 pm

NYU Students Apply Blockchain Solution to Electronic Voting Security

December 9, 2016, 11:00 am

Old Linux Kernel Code Execution Bug Patched

December 8, 2016, 9:15 am

Sony Closes Backdoors in IP-Enabled Cameras

December 6, 2016, 11:24 am

Distributed Guessing Attack Reels in Payment Card Data

December 5, 2016, 2:10 pm

Mozilla Patches Firefox Zero Day Used to Unmask Tor Browser Users

December 1, 2016, 12:00 pm

Tor Patched Against Zero Day Under Attack

November 30, 2016, 12:44 pm

Hackers Make New Claim in San Francisco Transit Ransomware Attack

November 28, 2016, 3:30 pm
ShadowBrokers Selling Windows Exploits, Attack Tools | Threatpost | The first stop for security news

Microsoft Patches Zero Day Disclosed by Google
November 8, 2016, 2:57 pm

Microsoft Says Russian APT Group Behind Zero-Day Attacks
November 1, 2016, 5:50 pm

Google to Make Certificate Transparency Mandatory By 2017
October 29, 2016, 6:00 am

Microsoft Extends Malicious Macro Protection to Office 2013
October 27, 2016, 4:27 pm

Dyn DDoS Work of Script Kiddies, Not Politically Motivated Hackers
October 25, 2016, 3:00 pm

Mirai-Fueled IoT Botnet Behind DDoS Attacks on DNS Providers
October 22, 2016, 6:00 am

Dyn Confirms DDoS Attack Affecting Twitter, Github, Many Others
October 21, 2016, 10:01 am

FruityArmor APT Group Used Recently Patched Windows Zero Day
October 20, 2016, 7:00 am

Experts ‘Outraged’ by Warrant Demanding Fingerprints to Unlock Smartphones
October 18, 2016, 4:58 pm

Leftover Factory Debugger Doubles as Android Backdoor
October 14, 2016, 9:00 am

IoT Botnets Are The New Normal of DDoS Attacks
October 5, 2016, 8:51 am

Researchers Break MarsJoke Ransomware Encryption
October 3, 2016, 5:00 am

OpenSSL Fixes Critical Bug Introduced by Latest Update
September 26, 2016, 10:45 am

500 Million Yahoo Accounts Stolen By State-Sponsored Hackers

https://threatpost.com/shadowbrokers-selling-windows-exploits-attack-tools/123027/
Yahoo Reportedly to Confirm Breach of Hundreds of Millions of Credentials

September 22, 2016, 12:31 pm

Experts Want Transparency From Government’s Vulnerabilities Equities Process

September 20, 2016, 2:41 pm

Bruce Schneier on Probing Attacks Testing Core Internet Infrastructure

September 15, 2016, 11:15 am

Generic OS X Malware Detection Method Explained

September 13, 2016, 9:14 am

Patched Android Libutils Vulnerability Harkens Back to Stagefright

September 9, 2016, 2:06 pm

Chrome to Label Some HTTP Sites ‘Not Secure’ in 2017

September 8, 2016, 3:43 pm

Threatpost News Wrap, September 2, 2016

September 2, 2016, 9:00 am

Insecure Redis Instances at Core of Attacks Against Linux Servers

September 1, 2016, 1:08 pm

Dropbox Forces Password Reset for Older Users

August 29, 2016, 9:58 am

Cisco Begins Patching Equation Group ASA Zero Day

August 24, 2016, 5:53 pm

New Collision Attacks Against 3DES, Blowfish Allow for Cookie Decryption

August 24, 2016, 8:00 am

Cisco Acknowledges ASA Zero Day Exposed by ShadowBrokers

August 17, 2016, 4:06 pm

Pokémon GO Spam, Ransomware, On the Rise

August 17, 2016, 12:58 pm
ProjectSauron APT On Par With Equation, Flame, Duqu
August 8, 2016, 1:40 pm

Miller, Valasek Deliver Final Car Hacking Talk
August 4, 2016, 3:26 pm

Researchers Go Inside a Business Email Compromise Scam
August 4, 2016, 10:00 am

Export-Grade Crypto Patching Improves
August 3, 2016, 10:00 am

Kaspersky Lab Launches Bug Bounty Program
August 2, 2016, 9:00 am

Threatpost News Wrap, July 29, 2016
July 29, 2016, 10:45 am

KeySniffer Vulnerability Opens Wireless Keyboards to Snooping
July 26, 2016, 9:30 am

Upcoming Tor Design Battles Hidden Services Snooping
July 25, 2016, 3:51 pm

EFF Files Lawsuit Challenging DMCA’s Restrictions on Security Researchers
July 21, 2016, 1:18 pm

Oracle Patches Record 276 Vulnerabilities with July Critical Patch Update
July 20, 2016, 9:21 am

Threatpost News Wrap, July 15, 2016
July 15, 2016, 11:00 am

Academics Build Early-Warning Ransomware Detection System
July 14, 2016, 1:05 pm

xDedic Hacked Server Market Resurfaces on Tor Domain
July 12, 2016, 11:40 am

Conficker Used in New Wave of Hospital IoT Device Attacks

https://threatpost.com/shadowbrokers-selling-windows-exploits-attack-tools/123027/
June 30, 2016, 11:48 am

655,000 Healthcare Records Being Sold on Dark Web

June 28, 2016, 10:00 am

Windows Zero Day Selling for $90,000

May 31, 2016, 5:44 pm

Millions of Stolen MySpace, Tumblr Credentials Being Sold Online

May 31, 2016, 1:37 pm

OTR Protocol Patched Against Remote Code Execution Flaw

March 10, 2016, 10:23 am

Clever Facebook Hack Reveals Private Email Address of Any User

December 23, 2016, 5:19 pm

PHPMailer Bug Leaves Millions of Websites Open to Attack

December 27, 2016, 1:22 pm

Google Removing SHA-1 Support in Chrome 56

November 17, 2016, 3:39 pm

Uber Portal Leaked Names, Phone Numbers, Email Addresses, Unique Identifiers

November 23, 2016, 10:00 am

WordPress Plugins Leave Black Friday Shoppers Vulnerable

November 22, 2016, 9:55 am

Exploit Code Released for NTP Vulnerability

November 22, 2016, 10:30 am

Android Trojan Switcher Infects Routers via DNS Hijacking

December 28, 2016, 4:00 am

ShadowBrokers Bid Farewell, Close Doors

January 12, 2017, 1:49 pm
Happy New Year from Central Moscow!...

Happy New Year folks, and hope you all had great holidays! You won’t believe this… but this post is about… RED SQUARE! // Incidentally, the square I consider to be the most beautiful spot ...

The “EyePyramid” attacks...

On January 10, 2017, a court order was declassified by the Italian police, in regards to a chain of cyberattacks directed at top Italian government members and institutions. The attacks leveraged a ma...

Quiz: Are you a likeaholic?

What would you do to get more likes on a social network? Take our quiz and see if you’re hooked on likes.
Star Wars: the Empire state of cybersecurity probl...

As you probably know, Star Wars: Rogue One has hit the theaters to tell the story of the Rebellion who steal the plans of Death Star and facilitate its destruction. The majority of viewers think that ...

Read more...

Kaspersky Academy attended MIT (IC)3 Annual Confer...

72 guests, among them a global security lead Gordon Morrison, attended the MIT (IC)3 Annual Conference to share the latest insights into the industry. Educational programs manager Christel Gampig-Avil...

Read more...