# Threatpost | The first stop for security news


- Categories
  - Category List
    - Cloud Security
    - Critical Infrastructure
    - Cryptography
    - Government
  - Category List
    - Hacks
    - Malware
    - Mobile Security
    - Privacy
  - Category List
    - SAS
    - Vulnerabilities
    - Web Security
  - Authors
    - Michael Mimoso
    - Christopher Brook
  - Additional Categories
    - Slideshows
  - The Kaspersky Lab News Service
- Featured
  - Authors
    - Michael Mimoso
    - Christopher Brook
  - The Kaspersky Lab News Service


## Featured Posts

All


Major Vulnerability Found In Schneider Electric…


Following Lull, New Campaigns Pushing Retooled…


Apple Patches iOS Flaw Exploitable by…


- Podcasts


## Latest Podcasts

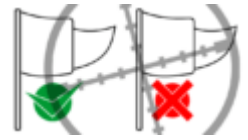
All

Threatpost News Wrap, October 21, 2016

Threatpost News Wrap, October 14, 2016


Gary McGraw on BSIMM7 and Secure…

Threatpost News Wrap, October 7, 2016


Juan Andres Guerrero-Saade and Brian Bartholomew…

Threatpost News Wrap, September 30, 2016

## Recommended

The Kaspersky Lab Security News Service

- Videos

## Latest Videos

All


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…


Santiago Pontiroli and Roberto Martinez on…

## Recommended

The Kaspersky Lab Security News Service

# ShadowBrokers Dumps Lists of Equation Group Hacked Servers

 by Michael Mimoso October 31, 2016 , 1:50 pm

The ShadowBrokers' last two bits of outreach to the world lacked the oomph of August's showstopper dump of Equation Group zero days, but the group is more than making up for it in severely broken English political banter, and another plea to buy the full boat of NSA exploits it allegedly has stolen.

The group posted a scattered message last night that included links to downloads of lists of hacked Sun Solaris and Linux servers that the Equation Group allegedly compromised and used to launch attacks.

## Related Posts

**Remote Code Execution Vulnerabilities Plague LibTIFF Library**

October 26, 2016 , 12:34 pm

**Adobe Patches Flash Zero Day Under Attack**

October 26, 2016 , 11:24 am

**[Lawmakers Asking What ISPs Can Do About DDoS Attacks](#)**

October 26, 2016 , 11:00 am

The pwned servers are old; the list ranges from 2001 to 2010. Most of the IP addresses of compromised servers are in Iran, Russia, China, Pakistan, India, Japan, South Korea, Bosnia and elsewhere.

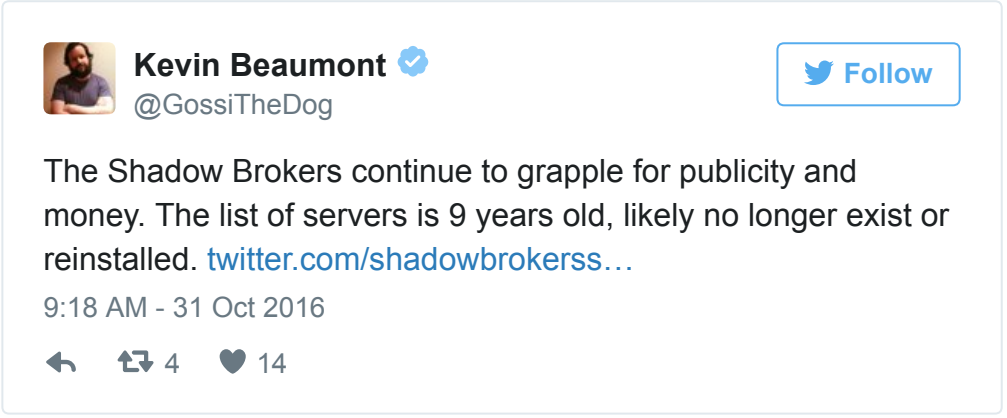
Researcher Matt Suiche, founder of a UAE security startup called Comae, analyzed the files and found 331 IP addresses compromised by a pair of spy tools called Intonation and PitchImpair.

"There's not much to see," Suiche told Threatpost, adding that most of the folders in the dumps contain metadata and some configuration variables. "There's no source code this time. It's not that significant as a leak."

The group claims that "many missions" were carried out from these compromised machines, and renewed its pitch for someone to buy the auction file of Equation Group exploits put up for bid in August.

"Maybe tools no more installed? Maybe is being cleaned up? To peoples is being owner of pitchimpair computers, don't be looking for files, rootkit will self destruct," the note says.

Experts believe this message, like its last one, is another plea for attention from the ShadowBrokers. In a Pastebin message earlier this month, the group complained about a lack of interest—and bidding—on the files it put up for auction. As of this afternoon, there has been minimal movement since August; currently the bid is 2.006074 Bitcoin, or roughly $1,414.




The ShadowBrokers' note starts off as an ode to the political rhetoric over alleged Russian interference with the U.S. presidential election, and intimating that they are offended that the CIA and not the NSA is threatening retaliation. "Where is the cyber A-Team?" the note says. "Maybe threating is not being for external propaganda? Maybe is being for internal propaganda? Oldest control trick in book, yes? Waving flag, blaming problems on external sources, not taking responsibility for failures."

The note also rants about political corruption and its influence on the U.S. (or USSA) election with a veiled threat to hack or further disrupt next week's general election.

"Maybe peoples not be going to work, be finding local polling places and protesting, blocking , disrupting , smashing equipment, tearing up ballots? The wealthy elites is being weakest during elections and transition of power," the note says. "Is being why USSA is targeting elections in foreign countries. Don't beleiving? Remembering Iran elections? Rembering stuxnet? Maybe is not Russia hacking election, maybe is being payback from Iran?"

The Shadowbrokers emerged in August when it announced an auction of weaponized exploits belonging to the Equation Group, which Kaspersky Lab identified in February 2015 and other experts have linked to the NSA. The group claims to have hacked the Equation Group and if the auction earned the group 1 million Bitcoin, more files would be dumped unencrypted.

The group did post a 300MB file that included a number of attacks against Cisco, Juniper, Fortinet and other high end enterprise networking gear. While some of the files were old, the dump did send Cisco and other vendors racing to patch suddenly disclosed zero-day vulnerabilities.

Kaspersky Lab, meanwhile, did confirm that the Shadowbrokers' initial dump and its research on the Equation Group shared a "strong connection."



Categories: Government, Hacks

## Leave A Comment

Your email address will not be published. Required fields are marked *

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <s> <strike> <strong>`

Name

Email



Post Comment

Notify me of follow-up comments by email.

Notify me of new posts by email.

# Recommended Reads




October 26, 2016 , 12:34 pm
Categories: Vulnerabilities

## Remote Code Execution Vulnerabilities Plague LibTIFF Library

by Chris Brook

Three vulnerabilities, all which can lead to remote code execution, exist in the LibTIFF library.

Read more...



October 26, 2016 , 11:24 am
Categories: Vulnerabilities

## Adobe Patches Flash Zero Day Under Attack

by Michael Mimoso

Adobe released an emergency Flash Player update that patches a use-after-free vulnerability being exploited in targeted attacks.

Read more...



October 26, 2016 , 11:00 am
Categories: Government, IoT

## Lawmakers Asking What ISPs Can Do About DDoS Attacks

by Michael Mimoso

Sen. Mark Warner of Virginia wrote a letter to the heads of the FCC, FTC and DHS asking whether ISPs have the power to keep insecure connected devices off the public Internet.

Read more...

# Top Stories

### Dyn Confirms DDoS Attack Affecting Twitter, Github, Many Others

October 21, 2016 , 10:01 am

### 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

**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**

September 22, 2016 , 3:47 pm

**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**

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

**Backdoored D-Link Router Should be Trashed, Researcher Says**

September 29, 2016 , 4:04 pm

**Source Code Released for Mirai DDoS Malware**

October 3, 2016 , 10:58 am

**ShadowBrokers Dumps Lists of Equation Group Hacked Servers**

October 31, 2016 , 1:50 pm

**Facebook Debuts Open Source Detection Tool for Windows**

September 27, 2016 , 12:24 pm

**Microsoft Adds .NET Core, ASP.NET to Bug Bounty Program**

September 2, 2016 , 4:23 pm

**Popular Android App Leaks Microsoft Exchange User Credentials**

October 14, 2016 , 8:00 am

**Cisco Warns of Critical Flaws in Nexus Switches**

October 7, 2016 , 10:55 am

# The Final Say

From Kaspersky Blogs


**The Internet of Harmful Things....**

In the early 2000s I'd get up on stage and prophesize about the cyber-landscape of the future, much as I still do today. Back then I warned that, one day, your fridge will send spam to your micr...

Read more…


**[Kaspersky DDOS intelligence report for Q3 2016...]**

Interesting trend this quarter was the increased activity of DDoS botnets in Western Europe. For the first time in a year the TOP 10 most attacked countries included three Western European countries –...

Read more…


**[Do your online photos respect your privacy?]**

Photo files typically contain additional data on shooting conditions, including a geotag. What happens to this data when the photo is published online?

Read more…


**[Forrester names Kaspersky Lab a leader in endpoint...]**

Forrester Research interviewed vendors and customers to evaluate top endpoint security providers....

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…

Threatpost | The first stop for security news The Kaspersky Lab Security News Service
CategoriesBlack Hat | Cloud Security | Critical Infrastructure | Cryptography | Featured | Government | Hacks | IoT | Malware | Mobile Security | Podcasts | Privacy | Security Analyst Summit | Slideshow | Uncategorized | Videos | Vulnerabilities | Web Security

- RSS Feeds
- Home
- About Us
- Contact Us

## Authors

Michael Mimoso
Tom Spring
Christopher Brook



- | Terms of Service
- | Privacy