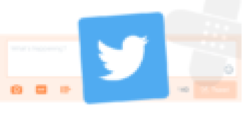
Threatpost | The first stop for security news

- 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

Android Overlay and Accessibility Features Leave…


Twitter Flaw Could Have Allowed Attacker…

Malware Network Communication Provides Better Early…

Latest Podcasts

All

Jaya Baloo on WannaCry and Defending…

[Threatpost News Wrap, May 19, 2017](#)

[Matthew Hickey on WannaCry Ransomware Outbreak](#)

[Threatpost News Wrap, May 12, 2017](#)

[Threatpost News Wrap, May 5, 2017](#)

[Threatpost News Wrap, April 28, 2017](#)

Recommended

[The Kaspersky Lab Security News Service](#)

- [Videos](#)

Latest Videos

[All](#)

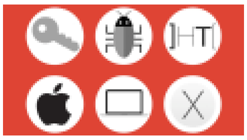
[iOS 10 Passcode Bypass Can Access…](#)

[BASHLITE Family Of Malware Infects 1…](#)

[How to Leak Data From Air-Gapped…](#)

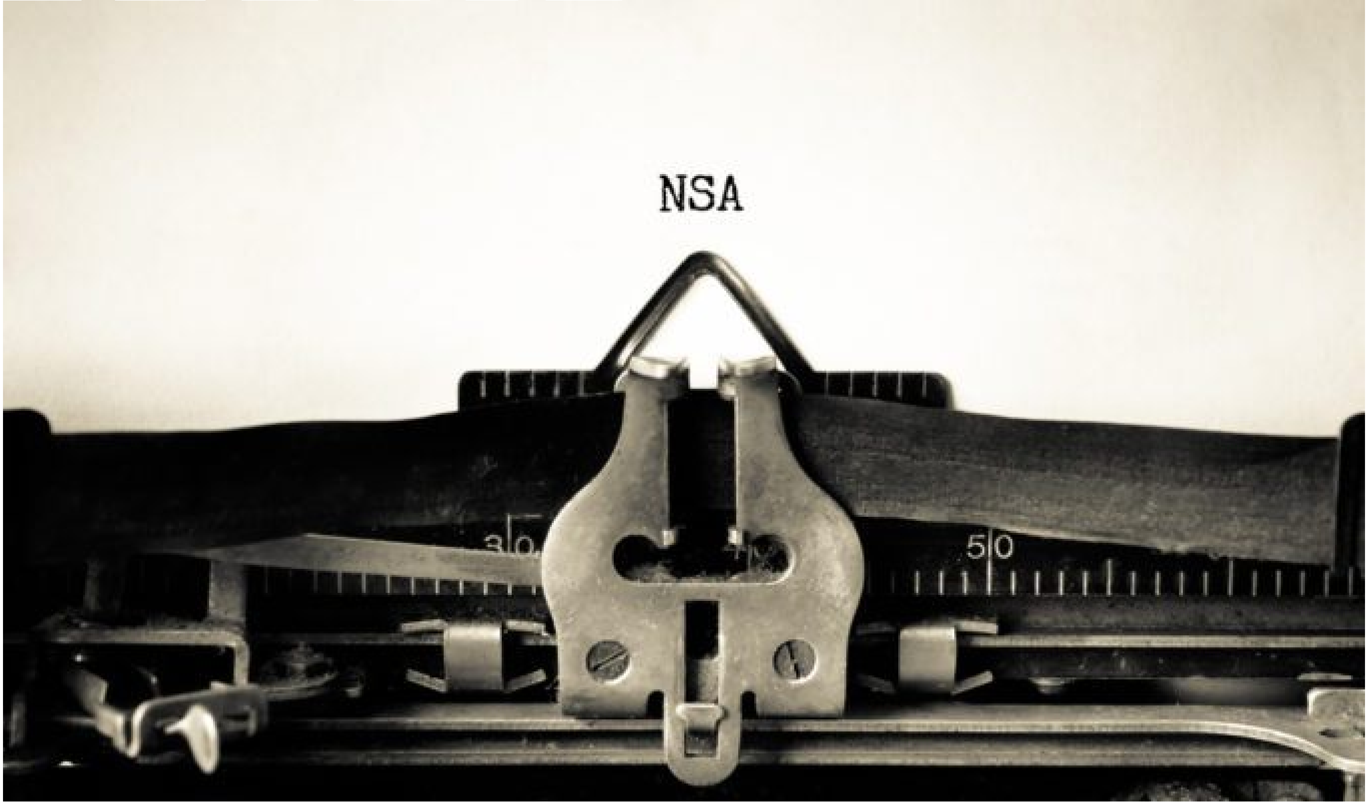
[Bruce Schneier on the Integration of…](#)

[Chris Valasek Talks Car Hacking, IoT,…](#)


[Patrick Wardle on OS X Malware…](#)

Recommended

[The Kaspersky Lab Security News Service](#)



EternalRocks Worm Spreads Seven NSA SMB Exploits

Follow @mike_mimoso by Michael Mimoso May 22, 2017 , 1:05 pm

Someone has stitched together seven of the Windows SMB exploits leaked by the ShadowBrokers, creating a worm that has been spreading through networks since at least the first week of May.

Researcher Miroslav Stampar, a member of the Croatian government's CERT, captured a sample of the worm last Wednesday in a Windows 7 honeypot he runs, and posted a report over the weekend on his Github page.

Related Posts

WannaCry Ransom Note Written by Chinese, English Speaking Authors

May 25, 2017 , 1:00 pm

Samba Patches Wormable Bug Exploitable With One Line Of Code

May 25, 2017 , 12:20 pm

Twitter Flaw Could Have Allowed Attacker to Tweet From Any Account

May 24, 2017 , 12:30 pm

The worm, which Stampar calls EternalRocks, currently has no payload and spreads in two stages over a 24-hour period. Heimdal Security has also seen a similar sample, which it calls BlueDoom.

Since the WannaCry ransomware outbreak two Fridays ago, researchers have stressed the urgency to patch the SMB vulnerability under attack given the NSA exploits are weaponized and documentation was also leaked making them reasonably simple to use. MS17-010 has been available since March, one month before the ShadowBrokers' leak of Equation Group Windows offensive hacking tools.

"Despite not having a malicious payload, the EternalRock worm is as complex as WannaCry – although, for now, less dangerous. Unlike WannaCry, however, EternalRock has two stages, and there's a long delay between the moment the malware sends a signal to the control server to confirm infection and the reply being received from the server," Kaspersky Lab said. "Such behavior is not unusual and seems to be a sandbox mitigation technique."

Stampar said that EternalRocks, which he also calls MicroBotMassiveNet, spreads using all of the SMB exploits in the leak, including EternalBlue, which was used in the WannaCry attacks. EternalRocks also uses EternalBlue, along with EternalChampion, EternalRomance and EternalSynergy, as well as ArchiTouch, SMBTouch and the DoublePulsar kernel exploit.

> Update on #EternalRocks. Original name is actually "MicroBotMassiveNet" while author's nick is "tmc" https://t.co/xqoxkNYfM7 pic.twitter.com/6Ico7gcg9u
>
> — Miroslav Stampar (@stamparm) May 19, 2017

"The analysis done on BlueDoom hints that cyber criminals may be preparing to integrate an array of different exploits for an attack that combines a full set of digital weapons," Heimdal Andra Zaharia said. "BlueDoom is different from WannaCry because it shows a long-term intent to make use of vulnerabilities stemming from virtually all Shadow Brokers leaks containing Windows exploits."

Stampar explained how the exploits attack in two stages. The first infects a vulnerable Windows machine unpatched against MS17-010, and the downloads components expected to be used during the second stage, along with the Tor browser, which is used to communication to a .onion command and control domain (ubgdgno5eswkhmpy[.]onion).

The second stage, Stampar said, is downloaded after a pre-defined 24-hour period from the .onion domain. During this stage, the SMB exploits are downloaded and the worm begins additional scanning of the internet looking for open instances of port 445.

Stampar's report includes indicators of compromises, including hashes of components used in both stages of the attack.

In the meantime, more information continues to surface about the WannaCry infections. To date, more than 200,000 infections have been recorded in more than 100 countries. According to researchers at Kaspersky Lab, 98 percent of WannaCry infections affected Windows 7 machines, primarily Windows 7 x64 machines.

> #WannaCry infection distribution by the Windows version. Worst hit – Windows 7 x64. The Windows XP count is insignificant. pic.twitter.com/5GhORWPQij
>
> — Costin Raiu (@craiu) May 19, 2017

Last week, researchers developed and published tools that can help admins recover the private encryption key used by WannaCry to encrypt files on the local drives of machines it infects.

Adrien Guinet of QuarksLab made available his WannaKey tool that is able to recover a prime number from memory used to factor the RSA public key stored by the malware on the local drive. That public key can be used to rebuild the private key and recover encrypted files in conjunction with another tool called WanaDecrypt, built by researcher Benjamin Delpy.

At first, the available tools were limited just to Windows XP machines. The attackers built WannaCry using the Windows Crypto API, which fails to overwrite the prime numbers in memory; later versions do so using the CryptReleaseContext function. Delpy was reportedly able to overcome that limitation and get his tool to work on Windows 7 machines as well.

Admins must now hold their breath waiting perhaps for a version of EternalRocks to spread a malicious payload. Already, the NSA's SMB exploits have been used, not only to spread ransomware, but also a cryptocurrency miner and a remote access Trojan. And unlike WannaCry, Stampar said EternalRocks does not include a so-called killswitch that researcher Marcus Hutchins used to shut down the initial ransomware outbreak.

"A big advantage over the initial WannaCry variants is that fact that EternalRock does not carry a kill-switch feature. Kaspersky Lab believes that it could easily be weaponized and used in the wild," Kaspersky Lab said.

This article was updated May 22 with comments from Kaspersky Lab.

f 0 g+ 14 in 0 0 💬 4

Categories: Malware, Vulnerabilities

Comments (4)

1. *Christian Schiffer* May 23, 2017 @ 8:50 am
   1

   In one way this is a good thing. See these exploits have existed for a while and have been used by malicious government entities to spy on us. The publication of these exploits and the consequential use of it by private malicious entities has helped focus on the problem and helped or forced the antivirus community to put an end to this treason.

   Reply ↓
2. *maounique* May 24, 2017 @ 5:14 am
   2

   Of course, this is a textbook case on why deliberately weakening security so the surveillance state can spy on everyone under the pretext of the war on islam, drugs, child porn, dissent, democracy and others which will undoubtedly be used by the official propaganda sooner or later cannot be accepted in any way shape or form, because nobody is perfect and, even if we accept the pretexts used, the backdoors will inevitably be leaked or sold to criminal organizations, maybe even the terrorists we were supposed to be protected from.

   Reply ↓
3. *Xian* May 24, 2017 @ 6:43 am
   3

   The good thing that came out of it, is at least now we know the government spying is a real thing and no myth or fable or make-believe. wannacry used like 2 of those hacks, this baby uses 7 so the only way to prevent it from occurring by switching to linux or at least updating your windows 10, updating your build of norton, kaspersky, eset or any decent antivirus and use a vpn like ivacy or pure or express to secure the data and log in from some region where malware attack is less frequent, at least for now. copy or become a victim because this thing's got no killswitch either. once it does make it to the pc, eternal rock may be a lot harder to stop compared to its daddy, wannacry

Reply ↓

4. *maounique* May 24, 2017 @ 10:02 am
   4

   “switching to linux”
   Linux is not and was never free of bugs. It is open source so backdoors are harder to introduce, but exploitable bugs are everywhere.
   Yes, it is way harder to subvert Linux but mostly because users are more informed and do not click on attachments and stuff, also because Windows is the low hanging fruit and much more standard as it is way harder to configure your own blend of OS, removing bloatware is notoriously difficult, so, attacking SMB in Windows is way easier since most Linux machines, even desktops, do not even have it installed, nevermind it is a different, reverse-engineered code implementation, sharing no code with the closed source windows one.

   Reply ↓

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

I'm not a robot
reCAPTCHA
Privacy - Terms

□ Notify me of follow-up comments by email.

□ Notify me of new posts by email.

Recommended Reads

f 0 8+ 6 in 0 0 0

May 25, 2017 , 1:00 pm
Categories: Malware

WannaCry Ransom Note Written by Chinese, English Speaking Authors

by Michael Mimoso

A linguistics analysis of the 28 ransom notes included with WannaCry indicate that native Chinese and English speakers wrote the original note, Flashpoint said.

Read more...

f 0 8+ 6 in 0 0 0

May 25, 2017 , 12:20 pm
Categories: Critical Infrastructure, Vulnerabilities, Web Security

Samba Patches Wormable Bug Exploitable With One Line Of Code

by Tom Spring

The Samba Team has patched a severe bug that leaves computers vulnerable to wormable exploit.

Read more...

f 0 8+ 3 in 0 0 0

May 24, 2017 , 12:30 pm
Categories: Featured, Vulnerabilities

Twitter Flaw Could Have Allowed Attacker to Tweet From Any Account

by Chris Brook

Twitter fixed a flaw in its Twitter Ads service could have allowed an attacker to tweet as any user.

Read more...

Top Stories

Jaya Baloo on WannaCry and Defending Against Advanced Attacks

May 22, 2017 , 9:00 am

Google Elevates Security in Android O

May 23, 2017 , 4:13 pm

Trump’s Cybersecurity Boss Talks Priorities

May 22, 2017 , 5:25 pm

Threatpost News Wrap, May 19, 2017

May 19, 2017 , 9:00 am

PATCH Act Calls for VEP Review Board

May 18, 2017 , 4:57 pm

VMware Patches Multiple Security Issues in Workstation

May 19, 2017 , 12:47 pm

Senate’s Use of Signal A Good First Step, Experts Say

May 18, 2017 , 12:05 pm

Fuze Patches Bug That Exposed Recordings of Private Business Meetings

May 2, 2017 , 9:05 am

The Final Say

From Kaspersky Blogs

Chanting ‘Issa-ee’ on the Kanda Matsuri....

In Tokyo on the weekend nearest the middle of May (this year – the 14th –15th) the Kanda Matsuri – aka the Kanda Festival – takes place every year. This is when all the residents of a district of Toky...

Read more…

Dridex: A History of Evolution...

In the several years that the Dridex family has existed, there have been numerous unsuccessful attempts to block the botnet’s activity. The ongoing evolution of the malware demonstrates that the cyber...

Read more…

How GDPR will affect your business

GDPR is just around the corner. Is your business prepared for it? Learn how others see GDPR and how it will change the world.

Read more…

How GDPR will affect your business

GDPR is just around the corner. Is your business prepared for it? Learn how others see GDPR and how it will change the world.

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

Authors

Michael Mimoso
Tom Spring
Christopher Brook

Copyright © 2017 Threatpost | The first stop for security news