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

 Microsoft Addresses NTLM Bugs That Facilitate…

 Adobe Fixes Six Vulnerabilities in Flash,…

 Micro Market Vendor Warns of Bankcard…

- Podcasts

Latest Podcasts

All

 Threatpost News Wrap, June 23, 2017

 Wikileaks Alleges Years of CIA D-Link…

 Threatpost News Wrap, June 16, 2017

 Patrick Wardle on MacRansom Ransomware-as-a-Service

 Threatpost News Wrap, June 9, 2017

 Threatpost News Wrap, June 2, 2017

Recommended

The Kaspersky Lab Security News Service

- Videos

Latest Videos

All

Mark Dowd on Exploit Mitigation Development


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,…

Recommended

The Kaspersky Lab Security News Service

Search

- Twitter
- Facebook
- Google
- LinkedIn
- YouTube
- RSS

Welcome > Blog Home>Vulnerabilities > Scanner Shows EternalBlue Vulnerability Unpatched on Thousands of Machines

Scanner Shows EternalBlue Vulnerability Unpatched on Thousands of Machines

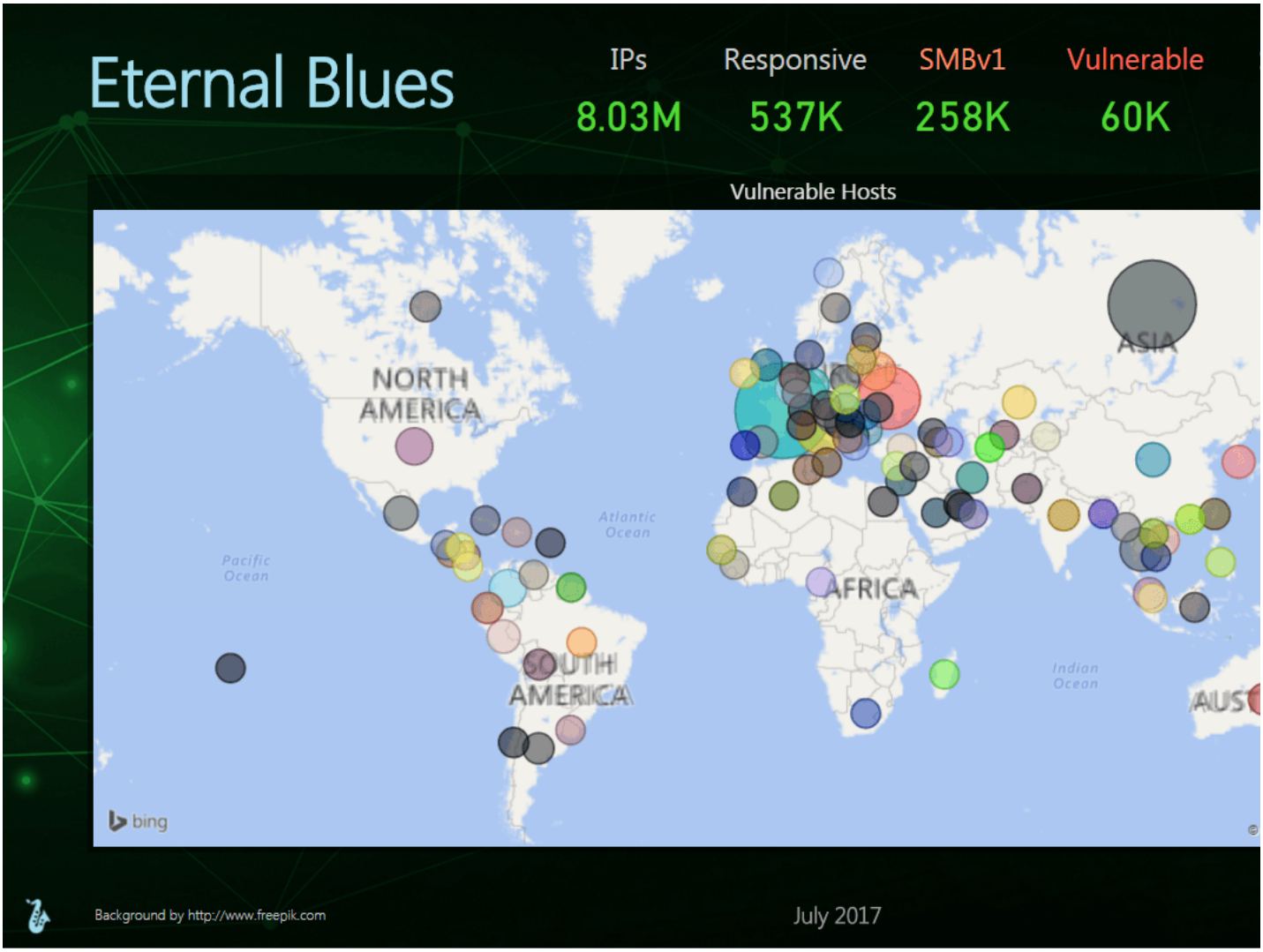
Follow @mike_mimoso by Michael Mimoso July 13, 2017 , 2:35 pm

Many digital trees have died for the cause of informing Windows admins about the SMBv1 vulnerability that spawned the WannaCry and ExPetr/NotPetya malware attacks. Yet a relatively small sample of data collected from a freely available tool shows that thousands have not gotten the message, or have some significant blind spots in their networks.

“There are always blind spots,” said Elad Erez, director of innovation at Imperva, who built the scanner called EternalBlues. “If you have 10,000 computers, can you really be that sure (that all hosts are patched)? You can’t. You need someone or something to help you with it.”

The scanner was made available in late June, and statistics collected from individuals and organizations that downloaded EternalBlues and ran it in their environments were published yesterday.

More than 8 million IP addresses (not hosts) were scanned by EternalBlues in 12 days, with 537,000 of those responding on port 445, the port over which SMB communication happens. Erez’s statistics show that 258,000 of those hosts were running the 30-year-old SMBv1 protocol, and 60,000 of those were vulnerable to the NSA’s EternalBlue exploit leaked by the ShadowBrokers.



WannaCry and ExPetr/NotPetya infected networks worldwide, with a heavy concentration of victimized machines in Russia and the Ukraine; Erez said one scan in the Ukraine uncovered 1,351 vulnerable hosts. WannaCry contained its own worming functionality in that once it infected machines, it began scanning the internet for other vulnerable hosts. ExPetr, meanwhile, was a wiper attack disguised as ransomware; the ransomware component of that attack was faulty and experts said it was clear the attackers never intended to decrypt compromised data or collect any money. Instead, the malware overwrote the Master Boot Record (MBR) on infected machines, leaving them useless.

Tools such as EternalBlues and others, Erez said, are vital for large networks, even those that may have applied the MS17-010 patch eradicating EternalBlue. One vulnerable endpoint is enough for either of these attacks to succeed. Erez said he built the tool for such a use case, as well as for smaller businesses that are unlikely to have IT or security teams responsible for patching or backups, the two strategies most important to countering ransomware attacks.

The results of the first 12 days of scan data surprised Erez.

“I thought it would be maybe 7 percent to 8 percent of hosts out there that would be vulnerable. It turned out to be 11 percent, a bit higher than I thought,” Erez said. “About one of nine hosts on the network is vulnerable. And who thought that more than half (53.9 percent) would still be open to this protocol?”

Awareness, however, may not be the entire cause, rather a lack of total visibility, especially into large enterprise networks, Erez said.

“People in the industry really know about the problem and are well aware that they need to mitigate it somehow. Running my tool, by definition, means they were well aware of the problem,” Erez said. “While there’s pretty good awareness from those who downloaded my tool, I don’t think [awareness] got to that second segment of users who are less sophisticated and don’t come from the tech industry—smaller businesses. I don’t think it made it to there. I really wanted to make this tool for smaller businesses who don’t have backups, who are more likely to pay, to help them before the next attack.”

Categories: Vulnerabilities

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

July 19, 2017 , 9:56 am
Categories: Malware

Modified Versions of Nukebot in Wild Since Source Code Leak

by Michael Mimoso

Criminals have made use of the leaked source code for the Nukebot banking Trojan, crafting modified versions of the malware to target banks in the U.S. and France.

Read more...

July 14, 2017 , 12:37 pm
Categories: Cryptography, Hacks, Malware, Web Security

NemucodAES Ransomware, Kovter Click-Fraud Malware Spreading in Same Campaigns

by Tom Spring

Researchers have spotted malicious email campaigns using Zip archives to spread NemucodAES ransomware and the Kovter click-fraud Trojan, simultaneously distributing both pieces of malware.

Read more...

July 14, 2017 , 10:00 am
Categories: Malware, Privacy, Vulnerabilities

Threatpost News Wrap, July 14, 2017

by Chris Brook

Mike Mimoso and Chris Brook discuss the news of the week, including the Verizon breach, the Oracle session hijacking attack, a Telegram-based hacking tool, and a free EternalBlue scanner.

Read more...

Top Stories

Siemens Patches Authentication Bypass Flaw in SiPass Server

July 14, 2017 , 12:37 pm

Oracle Releases Biggest Update Ever: 308 Vulnerabilities Patched

July 18, 2017 , 4:47 pm

SAP Patches High-Risk Flaws in SAP POS, Host Agent

July 12, 2017 , 12:25 pm

International Investigatory Group Also Target of Government Spyware

July 10, 2017 , 1:27 pm

Adobe Fixes Six Vulnerabilities in Flash, Connect with July Update

July 11, 2017 , 12:33 pm

Experts Warn Too Often AWS S3 Buckets Are Misconfigured, Leak Data

July 14, 2017 , 9:00 am

Cisco Patches Publicly Disclosed SNMP Vulnerabilities in IOS, IOS XE

July 14, 2017 , 11:01 am

Microsoft Extends Edge Bug Bounty Program Indefinitely

June 21, 2017 , 4:50 pm

The Final Say

From Kaspersky Blogs

A Sardinian Inn You Should Stay In. ...

Our north-to-south-to-north tour of Sardinia was coming to its logical end. But one final thing I really need to tell you about is the hotel we stayed at on our last night. It was the Hotel Cala di Vo...

Read more…

The NukeBot banking Trojan: from rough drafts to r...

This spring, the author of the NukeBot banking Trojan published the source code of his creation. Now, three months after the source code was published, we decided to have a look at what has changed in...

Read more…

Kaspersky Lab turns 20: Key events and milestones

Twenty years' worth of the most important events in the cybersecurity industry and Kaspersky Lab's history.

Read more…

Kaspersky Lab turns 20: Key events and milestones

Twenty years' worth of the most important events in the cybersecurity industry and Kaspersky Lab's history.

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