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

Svpeng Behind a Spike in Mobile…


Anthem Agrees to Settle 2015 Data…


New EU Privacy Laws Will Complicate…

- Podcasts

Latest Podcasts

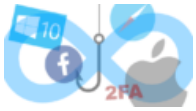
All


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

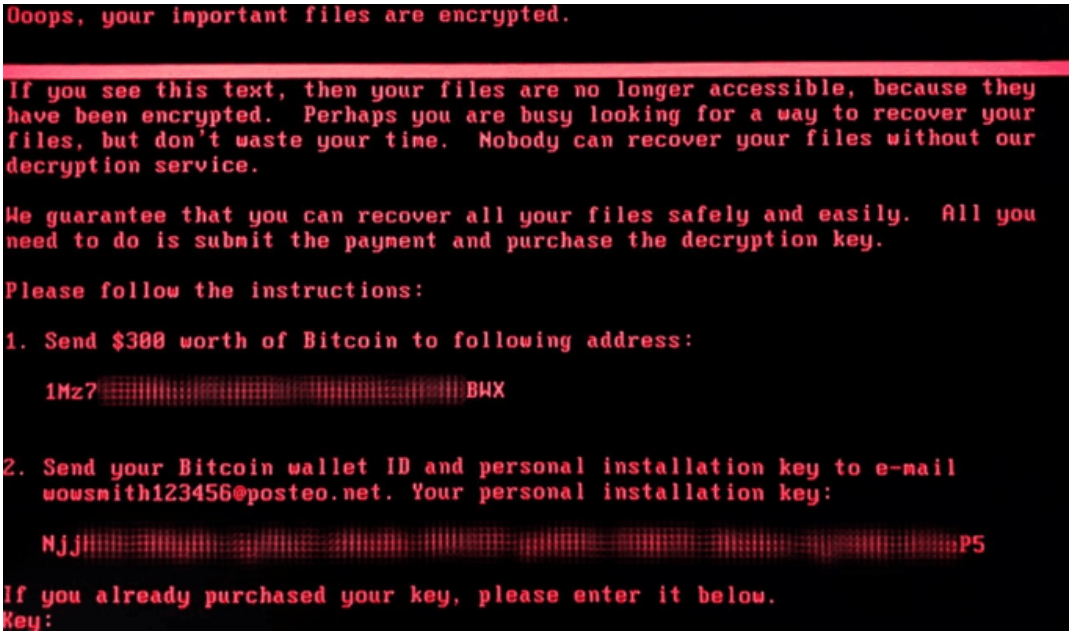
Search

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

-
-

Welcome > Blog Home>Malware > New Petya Distribution Vectors Bubbling to Surface

0 4 0 0 0



New Petya Distribution Vectors Bubbling to Surface

Follow @mike_mimoso by Michael Mimoso June 28, 2017 , 12:26 pm

Join Kaspersky Lab and Comae Technologies Thursday June 29, 2017 at 10 a.m. Eastern time for a webinar "The Inside Story of the Petya/ExPetr Ransomware." Click here to attend.

While Microsoft and others continue to shore up links between yesterday's global ransomware outbreak and the update mechanism for Ukrainian financial software provider MEDoc, others are finding even more distribution vectors used by the malware.

Kaspersky Lab last night said that a government website for the city of Bakhmut in Ukraine was compromised and used in a watering hole attack to spread the malware via a drive-by download.

"To our knowledge no specific exploits were used in order to infect victims. Instead, visitors were served with a malicious file that was disguised as a Windows update," Kaspersky Lab said in a statement. "We are investigating other leads in terms of distribution and initial attack vector."

The ransomware, which shares similarities to the destructive Petya strain that surfaced in 2016, is also being spread using the leaked NSA EternalBlue and EternalRomance exploits, infecting machines that still have not applied the MS17-010 Microsoft update that patches a handful of SMBv1 vulnerabilities targeted by the exploit. Unlike WannaCry, which had worming capabilities that allowed it to spread rapidly across the internet, this attack spreads itself only locally using a pair of Windows utilities, PSEXEC and WMIC, to do so, allowing it to infect machines patched against the vulnerabilities exploited by EternalBlue.

Like Petya, this attack overwrites the Master File Table and Master Boot Record on computers it infects. One organization reports that one unpatched machine was the culprit at its location, adding that it lost PCs due to a corrupted MBR, while other machines were showing the ransom note.

Researcher Matt Suiche of Comae Technologies said the malware is more wiper than ransomware, akin to Shamoon, the wiper malware behind the attacks on Saudi Arabia's Aramco oil company. Suiche said this malware destroys the first 25 sector blocks of a hard disk, and the MBR section of the disk is purposely overwritten with a new bootloader.

"The ransomware was a lure for the media, this version of Petya actually wipes the first sectors of the disk like we have seen with malwares such as Shamoon," Suiche wrote in an analysis published today. "The goal of a wiper is to destroy and damage. The goal of a ransomware is to make money. Different intent. Different motive. Different narrative."

Victims, meanwhile, continue to make payments in a futile attempt to recovery their lost hardware and data. German host Posteo said yesterday that it shut down the attacker's email account, wowsmith123456@posteo.net, which prevents victims from contacting the entity behind the attack in order to send them their Bitcoin wallet address and infection ID in order to verify payment of the $300 ransom.

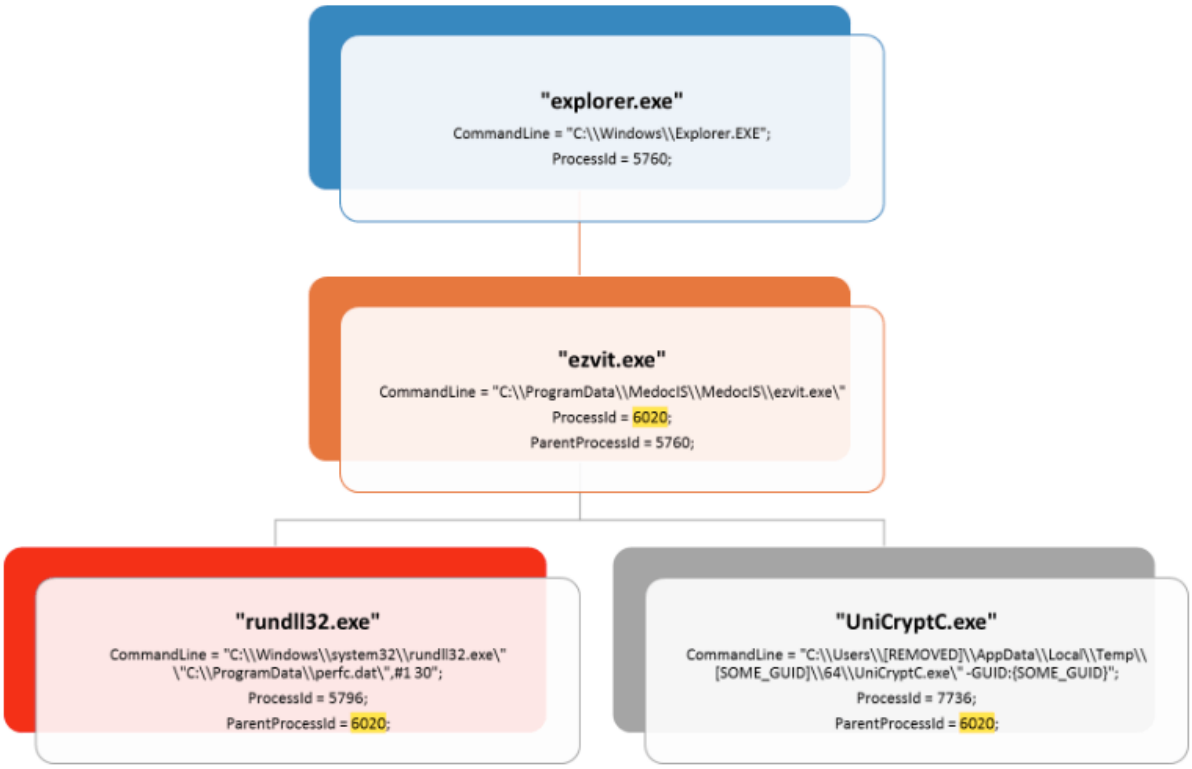
Microsoft, meanwhile, says it has definitively linked MEDoc as an initial infection vector, which MEDoc denied in a Facebook post Tuesday.

"The development team denies this information and argues that such conclusions are clearly erroneous, because the developer of m.e.doc, as a responsible supplier of the software, monitors the safety and cleanliness of its own code," MEDoc said.

MEDoc, which sells tax accounting software, was identified by Ukraine's Cyber Police as the source of the outbreak. Cisco and Kaspersky Lab also implicated the company, saying that its software update system had been compromised and was serving up the ransomware in phony updates.

"We observed telemetry showing the MEDoc software updater process (*EzVit.exe)* executing a malicious command-line matching this exact attack pattern on Tuesday, June 27 around 10:30 a.m. GMT.," Microsoft said in a Technet blog on Tuesday. Microsoft said that the EzVit.exe process from MEDoc executed the command line: *C:\\Windows\\system32\\rundll32.exe\" \"C:\\ProgramData\\perfc.dat\",#1 30*

Below is a representation of the execution chain from Microsoft.



The ransomware, which has been given many names including NotPetya, ExPetr, PetrWrap, GoldenEye and others, is much more complex than WannaCry given its ability to move laterally once on a local network.

Microsoft said the ransomware begins by dropping a credential-stealing tool similar to Mimikatz looking for valid admin or domain credentials. It then scans subnets looking for open port 445 or 139 connections.

"A special behavior is reserved for Domain Controllers or servers: this ransomware attempts to call *DhcpEnumSubnets()* to enumerate DCP subnets all hosts on all DHCP subnets before scanning for *tcp/139* and *tcp/445* services," Microsoft said. "If it gets a response, the malware attempts to copy a binary on the remote machine using regular file-transfer functionalities with the stolen credentials. It then tries to execute remotely the malware using either PSEXEC or WMIC tools."

Another scan looks for admin$ shares before the ransomware copies itself on the network and executes using PSEXEC in what amounts to pass-the-hash attacks, Microsoft said.

"In addition to credential dumping, the malware also tries to steal credentials by using the *CredEnumerateW* function to get all the other user credentials potentially stored on the credential store. If a credential name starts with *"TERMSRV/"* and the type is set as 1 (generic) it uses that credential to propagate through the network," Microsoft said. "This ransomware also uses the Windows Management Instrumentation Command-line (WMIC) to find remote shares (using *NetEnum/NetAdd*) to spread to. It uses either a duplicate token of the current user (for existing connections), or a username/password combination (spreading through legit tools)."

Experts continue to stress the importance of applying the MS17-010 update to unpatched machines, and advise disabling PSEXEC and WMIC on local networks.

Categories: Malware

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

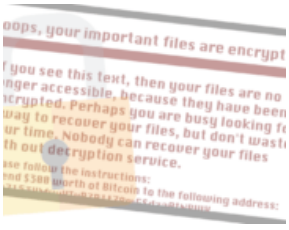
June 27, 2017 , 4:06 pm
Categories: Malware, Vulnerabilities

Complex Petya-Like Ransomware Outbreak Worse than WannaCry

by Michael Mimoso

Today's global ransomware attack is spreading via EternalBlue and through local networks using PSEXEC and WMIC.

Read more...



June 27, 2017 , 11:34 am
Categories: Critical Infrastructure, Government, Malware, Vulnerabilities

Second Global Ransomware Outbreak Under Way

by Tom Spring

A massive ransomware outbreak is spreading globally and being compared to WannaCry.

Read more...

June 26, 2017 , 1:54 pm
Categories: Vulnerabilities

Another RCE Vulnerability Patched in Microsoft Malware Protection Engine

by Michael Mimoso

Google Project Zero's Tavis Ormandy found another remote code execution vulnerability in the Microsoft Malware Protection Engine, the third since early May.

Read more...

Top Stories

Cisco Patches XXE, DOS, Code Execution Vulnerabilities

June 22, 2017 , 3:08 pm

Siemens Patches Vulnerabilities in SIMATIC CP, XHQ

June 23, 2017 , 2:07 pm

NSA-Backed OpenC2.org Aims to Defend Systems at Machine Speed

June 22, 2017 , 6:00 am

Microsoft Says Fireball Threat ‘Overblown’

June 22, 2017 , 1:11 pm

Average Cost of Breach Goes Down For the First Time Ever

June 22, 2017 , 1:51 pm

Few Victims Reporting Ransomware Attacks to FBI

June 23, 2017 , 1:34 pm

Second Global Ransomware Outbreak Under Way

June 27, 2017 , 11:34 am

Mexican Journalists, Lawyers Focus of Government Spyware

June 19, 2017 , 2:51 pm

The Final Say

From Kaspersky Blogs

Happy Birthday to Us – 20 Years Old – to the Day!...

Whoosh! What was that? That, boys and girls, was the history of cybersecurity passing by! 28 years ago, somewhere around the fall of 1989, my Olivetti M24 was attacked by a virus. That fateful event c...

Read more…

Schroedinger’s Pet(ya)...

Earlier today (June 27th), we received reports about a new wave of ransomware attacks spreading around the world, primarily targeting businesses in Ukraine, Russia and Western Europe. Our investigatio...

Read more…

New ransomware outbreak

A new ransomware outbreak is happening right now. Here's what we know so far and what you can do to protect yourself from the threat.

Read more…

New ransomware outbreak

A new ransomware outbreak is happening right now. Here's what we know so far and what you can do to protect yourself from the threat.

Read more…

Threatpost | The first stop for security news The Kaspersky Lab Security News Service
Categories Black 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