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


Apple Patches BroadPwn Bug in iOS…


Tor Project Opens Bounty Program To…


Bad Code Library Triggers Devil's Ivy…

Oracle Releases Biggest Update Ever: 308…


Microsoft Addresses NTLM Bugs That Facilitate…


Adobe Fixes Six Vulnerabilities in Flash,…

- Podcasts

Latest Podcasts

All

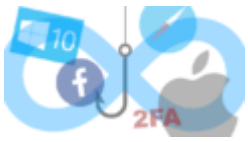
Black Hat USA 2017 Preview


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

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

Motivation Mystery Behind WannaCry, ExPetr

Follow @mike_mimoso by Michael Mimoso July 21, 2017 , 12:31 pm

If two is a coincidence and three is a trend, maybe we're not quite there yet in officially calling WannaCry and ExPetr a new movement among APT attacks. But for now, it's close enough.

Researchers are starting to examine the real motivations behind each global outbreak and whether these attacks truly signal a shift of direction in nation-state tactics.

Related Posts

macOS Fruitfly Backdoor Analysis Renders New Spying Capabilities

July 24, 2017 , 9:00 am

Modified Versions of Nukebot in Wild Since Source Code Leak

July 19, 2017 , 9:56 am

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

July 14, 2017 , 12:37 pm

Cisco's Midyear Cybersecurity Report seems to point in that direction, saying that attackers have destructive campaigns at scale in the works and that weakly protected and vulnerable connected devices are going to be vehicle for these attacks.

Kaspersky Lab, meanwhile, compared WannaCry and ExPetr side-by-side—both of which were spread entirely or in-part by the leaked NSA exploit EternalBlue—and warned that ransomware attacks are a pretty good shield for destructive attacks.

"One APT was rushed, opportunistic, not as technically capable as the other, while the other APT was practical, agile, and focused," Kaspersky Lab concluded about its WannaCry-ExPetr tale-of-the-tape. "But we are at the start of a trend emerging for this unusual tactic: APT camouflage destructive targeted activity behind ransomware."

ExPetr took that route, spreading ransomware that really wasn't profit-motivated malware. Errors in the code prevented recovery of data encrypted by the malware, which in concert with the actions of a German email host that shut down the attacker's email address left victims up a creek.

It didn't take long for researchers to conclude that ExPetr was instead a cloaked wiper attack foisted upon organizations in Ukraine primarily. Computers that were compromised by the malware had their Master Boot Record overwritten, rendering those machines lost forever, researchers said, adding that these were acts of sabotage and that collecting a few hundred dollars in Bitcoin from each victim was the furthest thing from the attackers' minds.

The difference between ExPetr and Shamoon, Destover or Black Energy is that those destructive attacks were much more aggressive and straightforward, Kaspersky Lab said.

"These components were all wiper technology, delivered in a very intentional and destructive manner. It's interesting that these spectacles all coincided with large political events and interests," Kaspersky Lab researchers said. "So this new need to cloak their destructive activity or sabotage is an interesting shared change in tactics."

WannaCry's well-documented killswitch was an odd choice to include in the ransomware, something that researchers still haven't completely figured out. Kaspersky Lab said it shared private reports with subscribing customers that indicate the attackers behind WannaCry also used spearphishing emails with links to files hosted at file-sharing services. The alleged resumes and job inquiries were instead executable files

that installed droppers and downloaders that were later used to install WannaCry. The attackers, alleged to be North Korea's Lazarus Group, did not attempt to collect the Bitcoin paid to recover files, nor did they enhance any development in the malware with features intent to turning a profit.

"This sort of inexpensive, two month long activity also may tell us a bit about the actor, their capabilities, and their interests — slow, practical, and somewhat hiding their interests in a very odd way," Kaspersky Lab said.

Cisco's report, meanwhile, focused more on the co-opting of IoT devices in large-scale attacks. The Dyn DDoS attacks of last fall showed the way, Cisco postulates, and now empowered by ExPetr, more may be on the way.

"There are signs that new types of attacks—more sinister and destructive than campaigns of the past—are in development. Adversaries are devising high-impact, wellplanned attacks that are designed to prevent any organization, big or small, from operating," Cisco said. "They know that no business has a contingency plan that outlines how to rebuild all their IT or OT from scratch, and they are determined to use that weakness to their advantage."

Categories: Malware

Comment (1)

1. *Posteo* July 23, 2017 @ 12:52 pm
   1

   Everything we already knew, and nothing new to add

   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

- [ ] Notify me of follow-up comments by email.
- [ ] Notify me of new posts by email.

Recommended Reads

July 24, 2017 , 9:00 am
Categories: Black Hat, Malware

macOS Fruitfly Backdoor Analysis Renders New Spying Capabilities

by Michael Mimoso

This week at Black Hat, Mac malware expert Patrick Wardle will describe how he used a custom-built command and control server to analyze new spying capabilities in a variant of the FruitFly backdoor.

Read more...

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...

Top Stories

FreeRADIUS Update Patches Bugs Static Analysis Tools Missed

July 17, 2017 , 2:09 pm

US, European Law Enforcement Shutter Massive AlphaBay Market

July 20, 2017 , 12:32 pm

Senator Calls For Use Of DMARC To Curb Phishing

July 19, 2017 , 3:46 pm

Threatpost News Wrap, July 14, 2017

July 14, 2017 , 10:00 am

Oracle E-Business Suite Flaw Allows Downloads of Documents

July 18, 2017 , 3:45 pm

macOS Fruitfly Backdoor Analysis Renders New Spying Capabilities

July 24, 2017 , 9:00 am

Modified Versions of Nukebot in Wild Since Source Code Leak

July 19, 2017 , 9:56 am

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

July 12, 2017 , 12:25 pm

The Final Say

From Kaspersky Blogs

KL AV for Free. Secure the Whole World Will Be....

Hi folks! I've some fantastic, earth-shattering-saving news: we're announcing the global launch of Kaspersky Free, which, as you may have guessed by the title, is completely free-of-charge...

Read more…

CowerSnail, from the creators of SambaCry...

We recently reported about SambaCry, a new family of Linux Trojans exploiting a vulnerability in the Samba protocol. A week later, Kaspersky Lab analysts managed to detect a malicious program for Wind...

Read more…

KL AV for Free. Secure the Whole World Will Be.

On July 25 – for our 20th birthday – Kaspersky Free will start being officially launched!

Read more…

KL AV for Free. Secure the Whole World Will Be.

On July 25 – for our 20th birthday – Kaspersky Free will start being officially launched!

Read more…

Authors

Michael Mimoso
Tom Spring
Christopher Brook

- | Terms of Service
- | Privacy