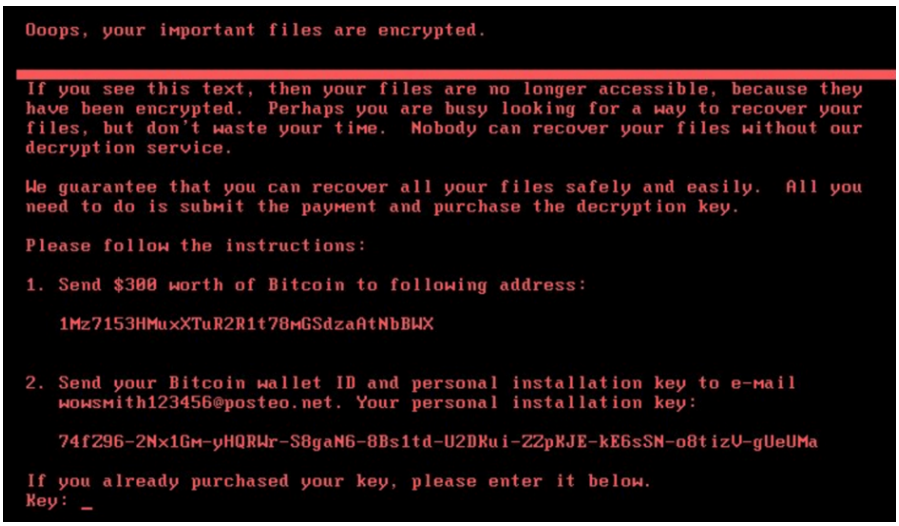
Krebs on Security

In-depth security news and investigation

27
Jun 17

‘Petya’ Ransomware Outbreak Goes Global

A new strain of ransomware dubbed “**Petya**” is worming its way around the world with alarming speed. The malware is spreading using a vulnerability in **Microsoft Windows** that the software giant patched in March 2017 — the same bug that was exploited by the recent and prolific WannaCry ransomware strain.



The ransom note that gets displayed on screens of Microsoft Windows computers infected with Petya.

According to multiple news reports, Ukraine appears to be among the hardest hit by Petya. The country’s government, some domestic banks and largest power companies all warned today that they were dealing with fallout from Petya infections.

Danish transport and energy firm **Maersk** said in a statement on its Web site that “We can confirm that Maersk IT systems are down across multiple sites and business units due to a cyber attack.” In addition, Russian energy giant Rosneft said on Twitter that it was facing a “powerful hacker attack.” However, neither company referenced ransomware or Petya.

Security firm **Symantec** confirmed that Petya uses the “Eternal Blue” exploit, a digital weapon that was believed to have been developed by the **U.S. National Security Agency** and in April 2017 leaked online by a hacker group calling itself the **Shadow Brokers**.

Microsoft released a patch for the Eternal Blue exploit in March (MS17-010), but many businesses put off installing the fix. Many of those that procrastinated were hit with the WannaCry ransomware attacks in May. U.S. intelligence agencies assess with medium confidence that WannaCry was the work of North Korean hackers.

Organizations and individuals who have not yet applied the Windows update for the Eternal Blue exploit should patch now. However, there are indications that Petya may have other tricks up its sleeve to spread inside of large networks.

Russian security firm **Group-IB** reports that Petya bundles a tool called "LSADump," which can gather passwords and credential data from Windows computers and domain controllers on the network.

Petya seems to be primarily impacting organizations in Europe, however the malware is starting to show up in the United States. *Legal Week* reports that global law firm **DLA Piper** has experienced issues with its systems in the U.S. as a result of the outbreak.

Through its twitter account, the **Ukrainian Cyber Police** said the attack appears to have been seeded through a software update mechanism built into M.E.Doc, an accounting program that companies working with the Ukranian government need to use.

Nicholas Weaver, a security researcher at the International Computer Science Institute and a lecturer at **UC Berkeley**, said Petya appears to have been well engineered to be destructive while masquerading as a ransomware strain.

Weaver noted that Petya's ransom note includes the same Bitcoin address for every victim, whereas most ransomware strains create a custom Bitcoin payment address for each victim.

Also, he said, Petya urges victims to communicate with the extortionists via an email address, while the majority of ransomware strains require victims who wish to pay or communicate with the attackers to use Tor, a global anonymity network that can be used to host Web sites which can be very difficult to take down.

"I'm willing to say with at least moderate confidence that this was a deliberate, malicious, destructive attack or perhaps a test disguised as ransomware," Weaver said. "The best way to put it is that Petya's payment infrastructure is a fecal theater."

Ransomware encrypts important documents and files on infected computers and then demands a ransom (usually in Bitcoin) for a digital key needed to unlock the files. With most ransomware strains, victims who do not have recent backups of their files are faced with a decision to either pay the ransom or kiss their files goodbye.

Ransomware attacks like Petya have become such a common pestilence that many companies are now reportedly stockpiling Bitcoin in case they need to quickly unlock files that are being held hostage by ransomware.

Security experts warn that Petya and other ransomware strains will continue to proliferate as long as companies delay patching and fail to develop a robust response plan for dealing with ransomware infestations.

According to **ISACA**, a nonprofit that advocates for professionals involved in information security, assurance, risk management and governance, 62 percent of organizations surveyed recently reported experiencing ransomware in 2016, but only 53 percent said they had a formal process in place to address it.

Update: 5:06 p.m. ET: Added quotes from Nicholas Weaver and links to an analysis by the Ukrainian cyber police.

Tags: Bitcoin, DLA Piper, Eternal Blue, Group-IB, ICSI, ISACA, Legal Week, Maersk, Microsoft Windows, MS17-010, Nicholas Weaver, petya, ransomware, Shadow Brokers, Symantec, UC Berkeley

46 comments

1. *Larry*
   June 27, 2017 at 4:35 pm

   Eternal Blue is based on a Windows vulnerability that the NSA discovered (or purchased) 5 years ago. They kept it secret, in spite of industry-government agreements to share information on vulnerabilities, because it was useful to them. It is doubtful that the intelligence benefit of keeping it secret outweighs the direct damage caused by keeping it secret, as well as the indirect damage to the reputation of the US. Just based on what has been affected so far it's highly likely that deaths will occur as a result of NSA's decision.

   Reply
   - *Jess tess*
     June 27, 2017 at 5:29 pm

     Larry, not necessarily true, nsa does discover exploits, but they also submit them to a "board" that includes industry (msft) and all come to a consensus on whether or not the exploit is "high priority". If eternal blue was never "set loose" in the wild, to this day no one would be the wiser.

     Reply
     - *A different Larry*
       June 27, 2017 at 10:41 pm

       To think no one would have found this vulnerability had it not been leaked is misguided at best. There are thousands, or more, well funded researchers out there that spend their life looking for these. To think the only people capable of finding something like this is the NSA borders on delusional. NOBUS risks lives, period.

Reply

- *Mick Maher*
  June 27, 2017 at 5:33 pm

  I was explaining Wannacrypt to my ten year old son a few weeks back in simplistic terms.

  He asked why didn't the spy company (the NSA) use the kill switch (register the domain) when they seen infection began to spread.

  I had no answer

  Reply

  - *David*
    June 27, 2017 at 5:45 pm

    That's because NSA did not develop WannaCry malware. They simply had (and accidentally leaked) the exploit that WannaCry used to infect network shares. NSA did not know about the Kill Switch domain… is was stumbled upon by a researcher. I think your (obviously smart) 10 year old can understand that.

    Reply

  - *vb*
    June 27, 2017 at 6:05 pm

    NSA developed the intrusion method, not the payload.

    Consider that NSA is the locksmith that opens the door. But they have nothing to do with the criminals that go through that door. Or what the criminal do once they are in.

    Reply

  - *art*
    June 27, 2017 at 6:07 pm

    They spy company didn't create the malware that spread around encrypting files. They created/bought a way to execute arbitrary code on a vulnerable system.
    This was used by another party to execute code that would encrypt files and ask for ransom. This party created the kill switch as part of their scheme.

    Reply

  - *Jess tess*
    June 27, 2017 at 7:17 pm

    Contrary to popular opinion, NSA isn't out there "looking" for this stuff..it comes to them and they conduct analysis.

    Reply

    - *stine*
      June 27, 2017 at 11:14 pm

      "… and they conduct analsys."

      And then what did they do? Call Microsoft 5 years later and say 'Hey, someone stole our attack database. You guys need to patch.'

      Reply

- *Alex*
  June 27, 2017 at 5:47 pm

  You blame the government for hiding it, why not blame the companies for failing to update their systems after being made aware after the fact? Just because it's a hassle, doesn't mean you blame the government.

  If they wouldnt update after, probably wouldnt had updated even if they were told up fron.t

  Reply

  - *Max A.*
    June 27, 2017 at 11:20 pm

    The companies that failed to update aren't even related to the comment that he made.

    Reply

    - *Mike S.*
      June 28, 2017 at 12:41 am

      Please read a bit better. The comment was attacking the original poster on his point. Yes, he didn't reference those companies and is blaming the NSA. The commenter is totally right that anyone who gets infected with this malware after

March 2017 has no right to blame the NSA since there has been a patch for the problem from that time. Should I blame Mircosoft for having buggy software even though they issued a patch for it and I failed to use it?

Reply

2. *Bruce Thompson*
June 27, 2017 at 4:37 pm

It's worth noting that Kaspersky is reporting that the email address in the ransom demand has been disabled by the provider in Germany, so there is no point at all in paying the ransom in this case.

Reply

3. *Pavlo Rodionov*
June 27, 2017 at 4:49 pm

One small notice. Not a National Bank (it's a separate organization), but some commercial banks. National Bank of Ukraine hasn't been affected by this attack.

Reply

4. *Greg Scott*
June 27, 2017 at 5:02 pm

Oh wow. We're early in analyzing this latest attack, but since it appears to use the same exploit as WannaCry, plus others, here is a link to a bunch of WannaCry information I collected you can use with end users.

http://dgregscott.com/ransomware-will-make-wannacry-can/

– Greg Scott

Reply

5. *Greg Scott*
June 27, 2017 at 5:05 pm

Oh wow – We're still early analyzing this latest attack, but since it apparently uses the same exploit as WannaCry, here is a link to a bunch of WannaCry information I collected for end users that should also be relevant to this attack.

http://dgregscott.com/ransomware-will-make-wannacry-can/

– Greg Scott

Reply

6. *Paul Cahill*
June 27, 2017 at 5:10 pm

Thanks for the article. I was piecing together this info from other news sites. Nice to have in one concise post.

Reply

7. *Greg Scott*
June 27, 2017 at 5:10 pm

Aw nuts! Sorry Brian – The first few times I posted my comment, nothing came back, even after refreshing. And now I see three of them posted. And I don't have a way to delete the extra ones.

– Greg

Reply

8. *Scott Schober*
June 27, 2017 at 5:14 pm

Great reporting Brian !

'Petya' ransomware makes me 'WannaCry'

Scott
http://www.HackedAgain.com

Reply

9. *Roberto Hellman*
June 27, 2017 at 5:17 pm

Nice Job! Brian
You are The Best Security Expert 100%
I am a Tech Guy myself and check out my Facebook

https://Facebook.com/roberto.hellman
and I am good friends with Leo Laporte

Reply

10. *James C*
June 27, 2017 at 5:17 pm

As always, KrebsOnSecurity on point. Thank you.

Reply

11. *Ulrik Holm Nielsen*
June 27, 2017 at 5:21 pm

Maersk confirms that they are hit by Petaya:
https://mobile.twitter.com/Maersk/status/879810135467720705/photo/1

The Danish news channel TV2 reported earlier today that the top management was assembled in the "situation room" – so this is serious business.

Reply

12. *Greg Scott*
June 27, 2017 at 5:26 pm

I just like posting stuff so
I'll be cool -in my mind

-Greg

Reply

13. *IRS iTunes Card*
June 27, 2017 at 5:48 pm

Interesting Read

Reply

14. *Leigh MS*
June 27, 2017 at 5:52 pm

While my kids complain that we don't have Windows OS at home I am so glad that we use Linux. Mostly use it at work as well. Integration and file sharing can be a bit of a hassle at times, but worth it. Yes there are occasional exploits, but nothing on this scale.
Not wishing to come over as smug, just relieved.

Reply

- *vb*
June 27, 2017 at 6:13 pm

I won't even let my kids use Linux. They use Chromebooks.

I can "Powerwash" in less than a minute. Even if the OS could be hacked, I can reload the OS from a USB drive in five minutes.

Reply

  - *Dave*
June 28, 2017 at 3:48 am

Chromebooks are based on Linux.

Reply

  - *Joey*
June 28, 2017 at 5:16 am

Love my Chromebook!

Reply

- *Andy*
June 28, 2017 at 3:53 am

Infection is usually a case of scale and profit, and as Linux catches up in terms of industry use, so does the malware:
https://blog.knowbe4.com/web-hosting-provider-pays-1-million-to-ransomware-attackers

Reply

15. *Chris*
June 27, 2017 at 6:03 pm

Looks like the kill switch was found about 90mins ago
by Amit Serper (@0xAmit)
https://twitter.com/0xAmit/status/879789734469488642

“Create a file called perfc with no extension in %windir%”

I can’t confirm.

Reply

16. *Paul DeGeiso*
June 27, 2017 at 6:53 pm

I’ve heard that kill switch is not reliable info or didn’t work for some. Vet all potential solutions carefully

Reply

- *JJ*
June 27, 2017 at 9:34 pm

The file name needs to be the same as the name of the DLL file it dropped on that computer without an extension. EternalBlue is #3 in the list of methods it uses to spread. It only uses it when the other two methods fail to allow it to spread laterally.

Reply

17. *GT500*
June 27, 2017 at 7:19 pm

A number of sources are saying that this appears to have originated in a malicious update to a Ukrainian accounting software called MeDoc that was published after an alleged attacker gained access to the network of the company that makes it:
https://www.bleepingcomputer.com/news/security/petya-ransomware-outbreak-originated-in-ukraine-via-tainted-accounting-software/

Reply

- *Michael R*
June 27, 2017 at 10:28 pm

Ironically, just last month Ukrainian president ordered a ban on competing accounting software company 1C (http://1c.ru/eng/). See http://www.economist.com/news/europe/21722360-blocking-websites-may-be-pointless-it-could-help-president-poroshenkos-popularity-ukraine, search for 1C.

Reply

18. *Victor L Hogg*
June 27, 2017 at 7:23 pm

Brian or anybody please.
I have been putting”CryptoPrevent on my clients’ computers now for about 10 months.
At it’s highest level of protection it prevents any program from being installed that tries to install executables in certain locations.
Does anybody have an opinion re: CryptoPrevent?

Reply

- *JCitizen*
June 27, 2017 at 8:16 pm

Most of what I know is that it prevented one ransomware attack in my honeypot lab. So I can attest it worked with at least one vector. We learned in MCSE school that the tools you can use in the Microsoft Management Console are a very powerful way to configure your system to use the best security practices available.

As I understand it, this is what CryptoPrevent does – it runs a batch file or script, that configures the MMC for the optimum settings (and I assume also snap-ins) to prevent unauthorized access, and hopefully also using encryption without permission.

I see no reason not to congratulate Foolish IT for coming up with the idea – most IT nerds don’t know half the settings they need to go through to do it themselves.

Reply

  - *Bruce Hobbs*
June 28, 2017 at 12:42 am

“I see no reason not to congratulate Foolish IT for coming up with the idea…”

How about “I congratulate Foolish IT for coming up with the idea…” You’re welcome.

Reply

19. *Mike*
June 27, 2017 at 7:54 pm

More recent analyses suggest that this malware variant is more sophisticated than originally thought. It attempts propagation via Psexec, WMI, and then EternalBlue
ref:
http://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html#more

Reply

20. *JCitizen*
June 27, 2017 at 8:03 pm

It must have been a slow news day in cable land – because they were all over the news with shrill shrieking, like the whole world was on fire – and that it just started today.

Good thing I can get the straight poop on Kreb's on Security! Thanks for the hard work Brian!

Reply

21. *Khalid*
June 27, 2017 at 8:06 pm

Can you please confirm the versaity of the said kill switch discovered by Amit Serper? Your expert opinion of the kill switch would be most valuable before I start deploying it system wide. Thank you!

Reply

22. *James Schumaker*
June 27, 2017 at 8:48 pm

I'm wondering if there is any information on who spread Petya. People in Ukraine I talk to think it's the Russians, and yet Rosneft is also affected. It would be extremely useful to know who the prime suspects are in this case, and what is being done to take them down.

Reply

23. *David A*
June 27, 2017 at 9:17 pm

The least surprising fact is that this attack has been refined and sculpted to be reused the most surprising is the sheer number of organisations, institutions and individuals who didn't take the warning of the original WannaCry and protect their Windows systems by upgrading. Sloppy! Some IT & security company heads will roll…

Keep up the good work Brian.

Reply

- *JJ*
June 27, 2017 at 9:45 pm

Not necessarily. The initial infection vector is not WannaCry (EternalBlue) this time. The malware downloads PsExec and tries to use it and WMIC to spread laterally (to other computers). It scans the local subnet, i.e. the one defined by the subnet mask of the infected PC. It only falls back to EternalBlue to spread itself id the other two methods have failed. You can be fully patched and still get nailed.

It also sets a scheduled task to reboot the infected computer one hour after infection to reload the now-encrypted Master Boot Record. This is just someone using the Ukraine and others for target practice in preparation for their real targets.

Reply

24. *fstx*
June 28, 2017 at 1:18 am

I want to thank the commenters providing substantial information about this, especially Mike. At the same time, I want to express my frustration with the commenters who must give their 2 paisa worth about Windows vs Linux, NSA, admin practices etc. 2 paisa is much much less than 2 cents.

Reply

25. *Ulrik Holm Nielsen*
June 28, 2017 at 3:06 am

To me the Petaya attack looks more like a deception to hide the real taget – Ukraine – than actually trying to make money from ransom. Why attack some of the largest company's in Europe and ask for petty 300 USD to unlock the computers?

Reply

26. *TABISH ASIFI*
June 28, 2017 at 4:04 am

FEW SIMPLE STEPS FOR IMMEDIATE DAMAGE CONTROL – https://www.linkedin.com/pulse/vaccinate-save-your-computer-network-against-petya-tabish?trk=v-feed&lipi=urn%3Ali%3Apage%3Ad_flagship3_me_share_analytics%3B0X6q92jC0%2Fqz3%2FSoE0u9AQ%3D%3D

Reply

Leave a comment

Name (required)

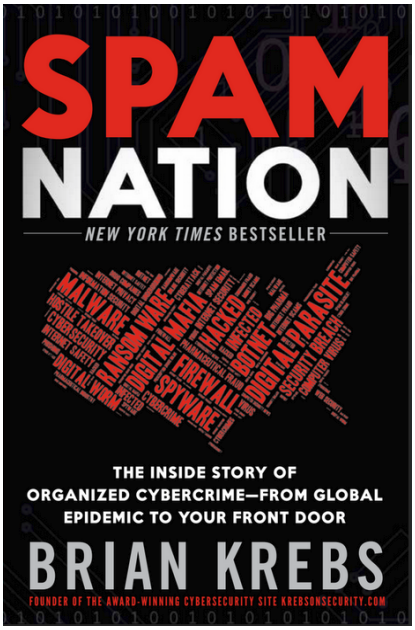
Email (required)

Website

Comment

Submit Comment

-
- ## My New Book!



A New York Times Bestseller!

- Buy at Amazon
- Donate with PayPal

- ## Recent Posts

  - ‘Petya’ Ransomware Outbreak Goes Global
  - Got Robocalled? Don’t Get Mad; Get Busy.
  - FBI: Extortion, CEO Fraud Among Top Online Fraud Complaints in 2016
  - Why So Many Top Hackers Hail from Russia
  - Credit Card Breach at Buckle Stores

- ## Subscribe by email

Please use your primary mailbox address, not a forwarded address.

Your email:
Enter email address...

Subscribe Unsubscribe

- ## All About Skimmers

Click image for my skimmer series.

- ## The Value of a Hacked PC

Badguy uses for your PC

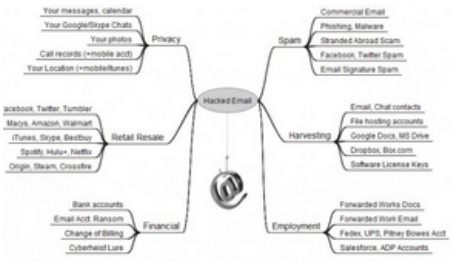
- ## Tools for a Safer PC

Tools for a Safer PC

- ## The Pharma Wars

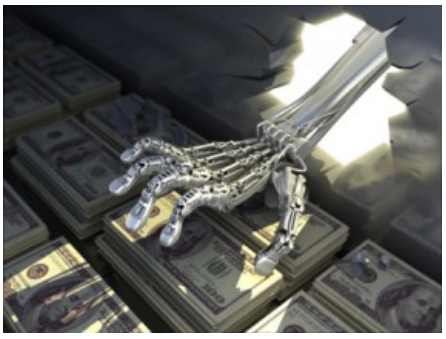
Spammers Duke it Out

- ## Badguy Uses for Your Email



Your email account may be worth far more than you imagine.

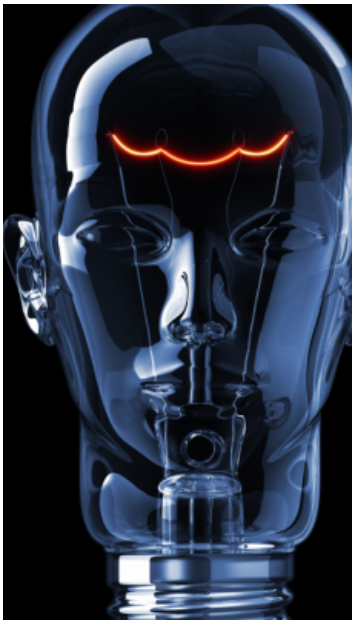
- ## eBanking Best Practices



eBanking Best Practices for Businesses

- ## Most Popular Posts

- ## Category: Web Fraud 2.0

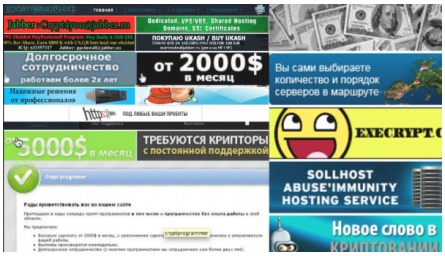


Innovations from the Underground

- 

ID Protection Services Examined

- **Is Antivirus Dead?**

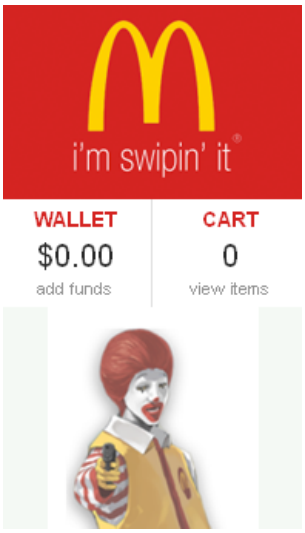


The reasons for its decline

- **The Growing Tax Fraud Menace**

File 'em Before the Bad Guys Can

- ## Inside a Carding Shop



A crash course in carding.

- ## Beware Social Security Fraud

Sign up, or Be Signed Up!

- ## How Was Your Card Stolen?

Finding out is not so easy.

- **Krebs's 3 Rules…**

...For Online Safety.
