

Forum:[Hack Forums](#)

Thread: [Petya Ransomware Spreads Rapidly Worldwide](#)

Xphile - June 27, 2017, 10:34 am

Incident Summary

According to multiple sources, a new variant of Petya ransomware, also known as Petwrap, is spreading rapidly with the help of same Windows SMBv1 vulnerability that the WannaCry ransomware abused to infect 300,000 systems and servers worldwide in just 72 hours last month.

(Source: [The Hacker News](#))

Damages Caused

(Above: Supermarket in Kharkiv, East Ukraine)

Petya ransomware has already infected — Russian state-owned oil giant Rosneft, Ukrainian state electricity suppliers, "Kyivenergo" and "Ukrenergo," in past few hours.

Kyivenergo's Press Service Wrote: "We were attacked. Two hours ago, we had to turn off all our computers. We are waiting for permission from Ukraine's Security Service (SBU) to switch them back on"

Additional Information & Further Reading

[Petya Ransomware Spreading Rapidly Worldwide, Just Like WannaCry - TheHackerNews](#)

[Petya Analysis / Detection Rate - VirusTotal](#)

[Petya Ransomware Bitcoin Address - Blockchain](#)

Updates

(Jun 27, 2017 11:20 AM)User1999 Wrote: [\[CITE\]](#) All those people that paid won't be getting their files back either. The company that the email is associated with shut down the email.

<https://posteo.de/blog/info-zur-ransomware-petrwrappetya-betroffenes-postfach-bereits-seit-mittag-gesperrt>

Google translate shows

At noon today we learned that Ransomware blackmail is currently providing a posteo address as a contact option.

Our abuse team checked this immediately - and the mailbox immediately blocked. We do not tolerate any misuse of our platform: The intermittent blocking of abused mailboxes is a normal procedure of providers in such cases. At the time of the blocking, there was no reporting on the Ransomware.

<https://mobile.twitter.com/GossiTheDog/status/879745509015072769>

(Jun 27, 2017 11:26 AM)MeanGene69 Wrote: [\[CITE\]](#) Source email address

The source email address is reported [2] as wowsmith123456@posteo.net with a filename Order-20062017.doc (RTF ?? CVE-2017-0199) [3]

Network Indicators of Compromise

The document results in a connection to 84.200.16.242 [3] and specifically /myguy.xls which is an HTA file. This results in connection to french-cooking[.]com. This drops another binary which results in:

111.90.139[.]247 80
COFFEINOFFICE[.]XYZ 80

Thanks for reading. ?

Papa Cuda - June 27, 2017, 10:36 am

Damn, they've docked quite the profit so far

Went up another \$300 in the time it took to post this

again....

Mr.Peanut - June 27, 2017, 10:39 am

(Jun 27, 2017 10:36 AM)?uda Wrote: [\[CITE\]](#) Damn, they've docked quite the profit so far

Went up another \$300 in the time it took to post this

2 bitcoins so far, I mean in the time frame maybe that's good but that's like \$4,600 right there. Definitely not worth it compared to the severity of the crime. Yes the people behind this are probably well tracked and it's Ukraine so maybe there in a nearby country with non extradition but still. Fuck ransomware lmao

Papa Cuda - June 27, 2017, 10:40 am

(Jun 27, 2017 10:39 AM)Mr.Peanut Wrote: [\[CITE\]](#) 2 bitcoins so far, I mean in the time frame maybe

that's good but that's like \$4,600 right there. Definitely not worth it compared to the severity of the crime. Yes the people behind this are probably well tracked and it's Ukraine so maybe there in a nearby country with non extradition but still. Fuck ransomware lmao

I agree, but I have a feeling in the next 24 hours that it will far surpass 2 BTC.

My guess.....

Spoiler [\(Click to View\)](#) 21 BTC

Xphile - June 27, 2017, 10:41 am

(Jun 27, 2017 10:36 AM)?uda Wrote: [\[CITE\]](#) - snip -

Shows the cost of not patching your machines before exposing them to the damn Internet. ???

Papa Cuda - June 27, 2017, 10:44 am

Gonna watch this closely, I'm interested as to how it will play out

jawsh33 - June 27, 2017, 10:45 am

Holy. Fuck. This shit is getting out of hand.

I remember making a crypto locker about a year ago, never intended to release it, but completely deleted the source code, because I didn't want to risk anything.

Edit: oh, and targeting supermarkets its fucking stupid, their computers are worth <300 & they have no info on it, it's all usually cloud based db's etc on their software.

Biker BoyZ - June 27, 2017, 10:47 am

Man this shit getting out of hand.

Riggs - June 27, 2017, 10:47 am

(Jun 27, 2017 10:41 AM)Ð3M0GORG0N Wrote: [\[CITE\]](#) Shows the cost of not patching your machines before exposing them to the damn Internet. ???

The costs are a lot more than that. Some businesses just adopt a "we will never pay" policy and refuse to foot the bill for company embarrassment.

Xphile - June 27, 2017, 10:51 am

(Jun 27, 2017 10:47 AM)Riggs Wrote: [\[CITE\]](#) The costs are a lot more than that. Some businesses just adopt a "we will never pay" policy and refuse to foot the bill for company embarrassment.

Very true, I assume it's mainly down to goodwill of the company and also the fact that the ransomware has no guarantee of sending a decryption key at all after payment.

I'm sure it's happened in the past where ransomware devs have no intentions of restoring systems after the ransom is paid.

Two more transactions, they've accumulated roughly \$ 5,951.78 (2.54183193 BTC) as of now.

Waiting to see how much this grows after 24 hours.

Papa Cuda - June 27, 2017, 10:56 am

(Jun 27, 2017 10:51 AM)Ð3M0GORG0N Wrote: [\[CITE\]](#) Very true, I assume it's mainly down to goodwill of the company and also the fact that the ransomware has no guarantee of sending a decryption key at all after payment.

I'm sure it's happened in the past where ransomware devs have no intentions of restoring systems

after the ransom is paid.

I mean the wannacry dudes seemed to be rather kind. I saw some thing were some guy in some third world country didn't have the money to pay so they gave him a key to unlock his computer anyway.

But yeah I would imagine that's not the case 99% of the time.

User1999 - June 27, 2017, 11:20 am

All those people that paid won't be getting their files back either. The company that the email is associated with shut down the email.

<https://posteo.de/blog/info-zur-ransomware-petrwrappetya-betroffenes-postfach-bereits-seit-mittag-gesperrt>

Google translate shows

At noon today we learned that Ransomware blackmail is currently providing a posteo address as a contact option.

Our abuse team checked this immediately - and the mailbox immediately blocked. We do not tolerate any misuse of our platform: The intermittent blocking of abused mailboxes is a normal procedure of providers in such cases. At the time of the blocking, there was no reporting on the Ransomware.

<https://mobile.twitter.com/GossiTheDog/status/879745509015072769>

MeanGene69 - June 27, 2017, 11:26 am

Source email address

The source email address is reported [2] as wowsmith123456@posteo.net with a filename Order-20062017.doc (RTF ?? CVE-2017-0199) [3]

Network Indicators of Compromise

The document results in a connection to 84.200.16.242 [3] and specifically /myguy.xls which is an HTA file. This results in connection to french-cooking[.]com. This drops another binary which results in:

111.90.139[.]247 80
COFFEINOFFICE[.]XYZ 80

jawsh33 - June 27, 2017, 11:27 am

(Jun 27, 2017 11:20 AM)User1999 Wrote: [\[CITE\]](#) All those people that paid won't be getting their files back either. The company that the email is associated with shut down the email.

<https://posteo.de/blog/info-zur-ransomware-petrwrappetya-betroffenes-postfach-bereits-seit-mittag-gesperrt>

Google translate shows

At noon today we learned that Ransomware blackmail is currently providing a posteo address as a contact option.

Our abuse team checked this immediately - and the mailbox immediately blocked. We do not tolerate any misuse of our platform: The intermittent blocking of abused mailboxes is a normal procedure of providers in such cases. At the time of the blocking, there was no reporting on the Ransomware.

<https://mobile.twitter.com/GossiTheDog/status/879745509015072769>

Yeah, I was so confused as to why they were using a posteo email adress haha.

So, they're just fucking stupid or what? RIP, this ransomware is fucking retarded.

Xphile - June 27, 2017, 11:53 am

(Jun 27, 2017 11:20 AM)User1999 Wrote: [\[CITE\]](#) All those people that paid won't be getting their files back either. The company that the email is associated with shut down the email.

<https://posteo.de/blog/info-zur-ransomware-petrwrappetya-betroffenes-postfach-bereits-seit-mittag-gesperrt>

Google translate shows

At noon today we learned that Ransomware blackmail is currently providing a posteo address as a contact option.

Our abuse team checked this immediately - and the mailbox immediately blocked. We do not tolerate any misuse of our platform: The intermittent blocking of abused mailboxes is a normal procedure of providers in such cases. At the time of the blocking, there was no reporting on the Ransomware.

<https://mobile.twitter.com/GossiTheDog/status/879745509015072769>

(Jun 27, 2017 11:26 AM)MeanGene69 Wrote: [\[CITE\]](#) Source email address

The source email address is reported [2] as wowsmith123456@posteo.net with a filename Order-20062017.doc (RTF ?? CVE-2017-0199) [3]

Network Indicators of Compromise

The document results in a connection to 84.200.16.242 [3] and specifically /myguy.xls which is an HTA file. This results in connection to french-cooking[.]com. This drops another binary which results in:

111.90.139[.]247 80
COFFEINOFFICE[.]XYZ 80

Thanks for the responses guys, I've added your contributions to the OP. ?

User1999 - June 27, 2017, 11:56 am

(Jun 27, 2017 11:27 AM)jawsh33 Wrote: [\[CITE\]](#) Yeah, I was so confused as to why they were using a posteo email adress haha.

So, they're just fucking stupid or what? RIP, this ransomware is fucking retarded.
I never even heard of posteo before this. Are they like a gmail for Germany?

Either way the results of this could be much more horrific than wannacry due to the fact no one now can decrypt their files. A huge shipping company and good amount of atms have been hit.

This is like a situation where do you let the email stay on your service to give people the ability to decrypt their files or not?

DigitalHighAss - June 28, 2017, 6:57 am

(Jun 27, 2017 11:56 AM)User1999 Wrote: [\[CITE\]](#) This is like a situation where do you let the email stay on your service to give people the ability to decrypt their files or not?

Allowing the attackers to keep that email will only encourage others to use that service again. Its a smart move to block them. In all reality there is no proof that paying the ransom would do anything either. They could just take the money and run. I just looked up the bitcoin address and they have about \$10,000 so far. No money moved out of that address.

Xphile - June 28, 2017, 7:02 am

(Jun 28, 2017 06:57 AM)DigitalHighAss Wrote: [\[CITE\]](#) Allowing the attackers to keep that email will only encourage others to use that service again. Its a smart move to block them. In all reality there is no proof that paying the ransom would do anything either. They could just take the money and run. I just looked up the bitcoin address and they have about \$10,000 so far. No money moved out of that address.

They appear to be getting some rather funny transactions though:

gdz\$ - June 28, 2017, 7:07 am

Jesus christ, not like this

jamdoughnut - June 28, 2017, 7:43 am

This is a bit of a strange one to be fair. Did you see the kill-switch? Seems a little simplistic in design. Word of the twitter verse is that it started off with a poisoned update to a financial software company (me-doc). Thing is the update came out like the day before it all kicked off. Either that's some next level development or that update was really poorly written.

Either way super interesting.

(Jun 27, 2017 11:20 AM)User1999 Wrote: [\[CITE\]](#) All those people that paid won't be getting their files back either. The company that the email is associated with shut down the email.

<https://posteo.de/blog/info-zur-ransomware-petrwrappetya-betroffenes-postfach-bereits-seit-mittag-gesperrt>

Google translate shows

At noon today we learned that Ransomware blackmail is currently providing a posteo address as a contact option.

Our abuse team checked this immediately - and the mailbox immediately blocked. We do not tolerate any misuse of our platform: The intermittent blocking of abused mailboxes is a normal procedure of providers in such cases. At the time of the blocking, there was no reporting on the Ransomware.

<https://mobile.twitter.com/GossiTheDog/status/879745509015072769>

The fact that the mail provider locked the entire account, denying them access to user decryption requests... Bit of a dick move really.

dismayed - June 28, 2017, 8:13 am

Here is the Malware analyst if anyone wants to look at it

<https://malwr.com/analysis/N2EwM2RjY2RkMDQwNDQwNjg2ZjM1OTNhOTY1YWE5NDA/>

n31ght0 - June 29, 2017, 1:50 am

So they just spreading by email? if so it's very easy to avoid this stuff. no worries even i use win 7

thesharp - June 29, 2017, 3:41 am

This is only the start I'm afraid they'll be a lot more to come with more zero day releases from shadow brokers premium customers.

Numinous - June 29, 2017, 3:45 am

You can prevent your system from Petya ransomware - <https://goo.gl/A9QKmW> (With 3 Methods)

veeeeeeeee4 - June 29, 2017, 11:53 am

This is cool, lets all use a type riter.

henixzer - June 29, 2017, 4:49 pm

So, does any one know from where(are they getting through shady downloads?) these people are getting infected by petya and wannacry?

AmericanExpress - June 29, 2017, 5:23 pm

(Jun 29, 2017 04:49 PM)henixzer Wrote: [\[CITE\]](#) So, does any one know from where(are they getting through shady downloads?) these people are getting infected by petya and wannacry? Malware authors tend to spread malicious software through e-mails, download websites, drive-by-downloads/exploits, etc. It pretty much evolves around user-interaction of some sort for someone to become infected and the attacker attempting to social engineer the victim is a big part to play in people becoming infected (increases chances of the victim allowing a UAC alert or even downloading and running the attachment in the first place).

If people were careful about how they behave online (e.g. while handling downloads and dealing with e-mails from untrusted senders) then there would be a let loss infections world-wide.

It doesn't take much for someone to stay clean without any Anti-Virus protection just by thinking before they do things.

Xphile - June 30, 2017, 3:20 am

(Jun 29, 2017 04:49 PM)henixzer Wrote: [\[CITE\]](#) So, does any one know from where(are they getting through shady downloads?) these people are getting infected by petya and wannacry?

They both exploit the SMBv1 flaw that made DoublePulsar (the NSA tool leaked by the Shadow Brokers) so dangerous. After the Ransomware creates a foothold on one unpatched server, it will spread across the local network via PSEXEC and WMIC.

Basically, unpatched web-facing servers are the main cause of infections here.

Hope this helped. ?

MeanGene69 - *June 30, 2017, 7:39 am*

Petya was pushed out through hijacked software updates via M.E. Docs which is an accounting software most prevalent in Ukraine.

I would suspect this is not the first time the company's servers have pushed out malware. Can anyone source this?

Cacao - *July 1, 2017, 3:54 pm*

would be interesting to see what happens next