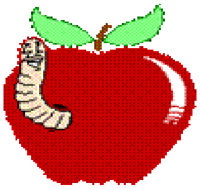
News from



The GLORIOUS SOCIETY OF THE WORMHOLE

April 2020

Hello Worms

This newsletter is early so my announcement gets early dissemination. The Glorious Society of The Wormhole meeting for April is cancelled. This virus stuff is too serious now to mess around and the age of our members makes us a vulnerable group. I recommend all to avoid groups of people as much as possible until this thing goes away. Stay home and burn a hotdog in your back yard. Check into the nets on Thursday.

I ask the officers and trustee to send me their normal meeting report at the end of the month. I will send out a “meeting newsletter” around the first Saturday.

All West Central Florida Section hamfests between now and the TARCFest on April 18 have been cancelled. I have not looked at the North or South Florida Sections. Most of you have probably already heard that Dayton is cancelled. I will not add or remove any hamfest to this newsletter at this time but think it will be a while before we see another hamfest.

The May Wormhole meeting will not be addressed until a later date as will the WormFest. Neither has a long lead time to do or cancel so there is no hurry to make any decision yet.

* NEW ROUTE TO YOUR COMPUTER FOR RANSOMWARE *

By Danny Palmer *ZDNet*

A ransomware campaign has returned with a new trick to fool the unwary into compromising their network with file-encrypting malware. And it's an attack that many Windows machines won't even recognize as potentially malicious.

The new variant of Paradise ransomware, which has been active in one form or another since 2017, spreads via phishing emails, but it's different from other ransomware campaigns because it uses an uncommon – but effective – file type to infiltrate the network. This campaign leverages Internet Query files (IQY), which are text files read by Microsoft Excel to download data from the internet. IQY is a legitimate file type, so many organizations won't block it.

But cybersecurity researchers at Lastline have uncovered a campaign taking advantage of this to spread Paradise ransomware to targeted organizations. "We're seeing attacks using IQY files because many commodity security products and automated systems do not, or cannot, parse these file types. Attackers realize they have a very good chance of making it past rudimentary defenses," Richard Henderson, head of global threat intelligence at Lastline, told ZDNet.

The initial phishing messages are designed to look commercial in nature and encourage users to open an IQY attachment. If the victim does this, the IQY file connects to the command and control server run by the attackers, which in turn will drop a PowerShell command that's used to execute the ransomware on the machine.

Once files are encrypted the victim is presented with a ransom demand – to be paid in cryptocurrency – in exchange for return to access to the network. In an effort to further understand the attack, researchers attempted to communicate with the cyber criminals through the chat 'support' channel they offer for negotiating access to a decryptor – although they never received a reply, indicating that the current campaign might only be a test run for more expanded distribution of the new version of Paradise. "Malware authors will often deploy malware that isn't quite ready for prime

time yet – they want to see how successful early versions of a new campaign are and how detectable their malware is against security products," said Henderson. The lack of 'support' response infers that they are still working out the kinks, and are trying to figure out the best ways for them to make money he added.
Cybersecurity researchers released a free decryption tool for a previous version of Paradise, but it appears that those behind the attacks are still pushing on.

It's not known what sort of cyber criminal operation is behind Paradise, although researchers note that the ransomware won't install on a machine if it detects the language ID as Russian, Kazakh, Belarusian, Ukranian, or Tatar.

* UPDATE - SOMEONE HIJACKED A HUGE BOTNET AND IS REMOVING IT*

By Catalin Cimpanu *ZDNet*

Microsoft announced today a coordinated takedown of Necurs, one of the largest spam and malware botnets known to date, believed to have infected more than nine million computers worldwide.

The takedown effort came after Microsoft and industry partners broke the Necurs DGA -- the botnet's domain generation algorithm, the component that generates random domain names.

Necurs authors register DGA-generated domains weeks or months in advance and host the botnet's command-and-control (C&C) servers, where bots (infected computers) connect to receive new commands.

"We were then able to accurately predict over six million unique domains that would be created in the next 25 months," said today Tom Burt, Microsoft Vice President for Customer Security & Trust.
Breaking the DGA allowed Microsoft and its industry partners to create a comprehensive list of future Necurs C&C server domains that they can now block and prevent the Necurs team from registering.

Breaking the DGA allowed Microsoft and its industry partners to create a comprehensive list of future Necurs C&C server domains that they can now block and prevent the Necurs team from registering.

Furthermore, Microsoft's legal team also intervened and obtained a court order last week, on March 5, granting Microsoft control over existing Necurs domains that were being hosted in the US.
"By taking control of existing websites and inhibiting the ability to register new ones, we have significantly disrupted the botnet," Burt said.

The OS maker said it worked with cybersecurity firms, internet service providers, domain registries, government CERTs, and law enforcement across 35 countries to coordinate the Necurs takedown, making this one of the biggest coordinated takedowns that have ever taken place.

After Microsoft has taken control of existing Necurs infrastructure, the company and its industry partners have been able to sinkhole the botnet and receive information about all the bots located across the world. As a final step part of this effort, Microsoft says it's now working with ISPs and CERT teams to notify users who have been infected so that they can remove the malware from their computers.

Historically, the Necurs botnet first appeared in 2012 and became one of the largest spam botnets known to date. The botnet is the collection of all computers that have been infected by a malware module named Necurs. The Necurs spam module runs on a user's computers and uses its resources to send out massive amounts of spam email on a daily basis.

According to Microsoft, during a recent 58-day investigation, its engineers tracked one single Necurs-infected computer sending out more than 3.8 million emails to more than 40.6 million victims.

The emails usually carry malware-laced attachments, but the Necurs is also used to spread pump-and-dump stock scams, fake pharmaceutical spam email and "Russian bride" dating scams.

The botnet is believed to be managed by the creators of the Dridex banking trojan, known as Evil Corp, charged last year by US authorities. But while Necurs has spewed out a lot of Dridex-infected spam emails, the botnet has also often rented its services to many other criminal gangs, carrying a wide assortment of other malware strains, including ransomware, remote access trojans, and information-stealing trojans.

Cybersecurity firm BitSight, which also played a crucial role in the takedown, has published today a report on Necurs' infrastructure before it was taken down.

* ANTENNA CAPTURE AREA*

What is it? Does it mean the bigger the antenna the more performance it will have.

A very large antenna that has not been resonated can receive and transmit very poorly. If you resonate the antenna by a tuner or other technique, it will become quite affective. The size of the antenna will have an effect.

Not everyone can put up BIG antennas. Therefore, how can you determine if the antenna has sufficient capture area?

Keep in mind, this is an "area", not length. A wire has little area per foot. Making long skinny antennas will give the capture area needed. However, at the same time it needs to be resonant somehow or it will not perform well and your radio will reject it.

So, do you want to use sheets of 4'X 8' plate steel for this "area"?

If you want you could, but there is a better way to determine if the antenna has enough capture to be affective.

Start with a very small resonant circuit. A capacitor and inductor in series. I am referring to components you would find on a circuit board. The circuit is resonant just like an antenna. Why would you not put this on your 60 foot tower? Because it would not impress anyone that tries to see it. It would not be impressive to anyone trying to hear it either, why?

A series resonant circuit using small components is certainly doing the same thing electrically as the big antenna. Except for one value that you can measure. Radiation resistance. A small circuit will have a radiation resistance close to zero ohms. This means it is close to a dead short. Or, it means the circuit will have to operate at a very high current. This plummets efficiency.

Try making the circuit bigger. Use a bigger coil and an air spaced capacitor. You are also increasing the radiating area of the antenna. If you measure the radiation resistance, you will find it has increased. It will also start to radiate more efficiently.

Keep increasing the physical area of the resonant circuit and you eventually achieve 25, 50, 100 ohms and higher. When you start to get radiation resistance readings at resonance of these values, the antenna becomes quite efficient.

For example, you make the coils and capacitor large enough to develop 50 ohms of radiation resistance. This is convenient since most radios match to 50 ohms. If you do this using only an inductor and large plated capacitor your efficiency can be figured as:

radiation resistance ÷ (radiation resistance + pure resistance)

Since your pure resistance is the resistance of the coil (using an ohm meter), it will be very close to zero or just a fraction of an ohm. This puts your efficiency almost to 100%.

Making the antenna bigger will offer little improvement since your efficiency is maxed out.

So, how big do you make it to have this 50 ohm radiation resistance?

It is sales pitch time. The sizes of the Isotrons are based on having enough "Capture Area" to develop 50 ohms of radiation resistance or more to provide a fully efficient antenna. It will be evident initially at the receiver, it will come alive. Putting the antenna in a good location will offer good transmit performance.

73,
Ralph WD0EJA
Bilal Company
MARCH 2020

* ZERO DAY BUG IN CHROME*

CLUB MEETING

There will not be a club meeting on April 4th due to the virus. We meet on the first Saturday every month at 11:00 Saturday morning at the Minnreg Building located at 6340 126th Ave N, Largo. Members are welcome to come in the rear area through the fence gate on the southeast corner of the property. Talk-in is on the Wormhole repeater system. For those coming to the meeting who cannot hit our repeater we will be monitoring the Honeywell club repeater on 443.050 +141.3. We will keep an eye peeled for you. We will take advantage of the cooking facilities with an after-the-meeting Social and Wormdog picnic.

CLUB NETS

Check in on the club net Thursdays at 1930 and 2000 (or at the end of the 2M net). 2M at 146.850 – with a tone of 146.2. Our 6M net runs after our regular 2M net on 53.150 – 1MHz offset 146.2 tone. We are always looking for volunteers to be the net control operator. Anyone interested, talk to one your club officers.

LOCAL NETS

MONDAY

1730 147.030 + Receiver sites and tone info http://www.qsl.net/wd4scd/ St Pete Yacht Club ARC

1830 147.060+ no tone St Pete ARC daily net St Petersburg

1900 144.210 USB CARS, vertical polarization Clearwater

1900 147.135 +146.2 Zephyrhills ARC Zephyrhills

2000 147.165+ 136.5 Brandon ARS from Brandon

2000 50.135 Pinellas ARK Pinellas County

2030 NI4CE system EAGLE Net, NTS traffic net, NI4CE system

2030 145.450 Pinellas ARK Pinellas County

TUESDAY

1830 147.060 no tone St Pete ARC daily net from St Petersburg

1900 50.200 USB 6M net Brandon ARS

1900 28.450 WCF section net Clearwater

1900 NI4CE system WCF Section VHF ARES NI4CE system

1930 145.170 & 442.4 both pl 156.7 Pinellas ACS net Clearwater

1930 444.900 +141.3 Sheriff’s Tactical ARC Tampa

2000 NI4CE system WCF Skywarn net NI4CE system

2000 147.105+ 146.2 Tampa ARC net from
Tampa

2000 28.365 USB simplex Brandon ARS

2030 NI4CE system EAGLE Net, NTS traffic net NI4CE
system

2100 28.465 USB 10/10 net from Orlando

1900 146.490 simplex 3RD Tuesday monthly, Hillsborough Co ARES
simplex Net

WEDNESDAY

1830 147.060 no tone St Pete ARC daily net from St
Petersburg

1930 52.020 simplex Suncoast 6'ers from St
Petersburg

1930 NI4CE system WCF Section Digital Info Ne NI4CE
system

2000 147.105 146.2 Greater Tampa CERT net from
Tampa

2000 146.97- 146.2 Clearwater ARS from
Clearwater

2030 NI4CE system EAGLE Net, NTS traffic net NI4CE
system

2100 NI4CE system Tampa Bay Traders Net non-
affiliated

THURSDAY

1800 146.52 simplex Hillsborough ARES/RACES North
Tampa

1830 147.060 no tone	St Pete ARC daily net	from St Petersburg
1900 444.750 +146.2	Fusion net	from Tampa
1915 224.660- no tone	St Pete ARC	from St Petersburg
1930 146.6385 -127.3	Lakeland ARC	from Lakeland
1930 444.225 + 146.2	Hillsborough ARES/RACES	from Tampa
1930 146.850- 146.2	Wormhole	from St Petersburg
2000 53.150 –1MHz 146.2	Wormhole	from St Petersburg
2030 NI4CE system	EAGLE Net, NTS traffic net	NI4CE system

FRIDAY

1830 147.060 no tone	St Pete ARC daily net	from St Petersburg
2030 NI4CE system	EAGLE Net, NTS traffic net	NI4CE system

SATURDAY

0730 3.940 (7.281 Alt.)+/- QRM	WCF Section HF Net	from WCF
1830 147.060 no tone	St Pete ARC daily net	from St Petersburg
2030 NI4CE system	EAGLE Net, NTS traffic net	NI4CE system

SUNDAY

0800	3.933	Florida Traders Net	non-affiliated
1830	147.060 no tone	St Pete ARC daily net	from St Petersburg
1930	NI4CE system	WCF Section Net	NI4CE system
2000	147.550 simplex	550 Simplex Net	Pinellas County
2030	NI4CE system	EAGLE Net, NTS traffic net	NI4CE system
2100	144.210 USB	Clearwater ARS	vertical orientation

FOR SALE / WANTED

Anyone having something for sale or who might be looking for an item let me know. I will not print phone numbers or email addresses unless specifically told to since this newsletter might end up on the web. The exception is when I get the information off the web. If you are a member of the Wormhole then you have all the information you need on a club roster and if you are not a member .. why not? OK, if you are not a member you can contact me at the email address at the end of this newsletter, I will give you the information to contact the person involved.

FOR SALE, ICOM **IC-756 Pro**, HF and 6M, 100 watts, hand mic, power cord and manual, Local only. See George W1AAG

HAMFESTS

April 18	**TARCFest** TARC Clubhouse, 22nd St at the river, $5 entry including tailgate, a few inside tables reserved in advance, talkin on 147.105 +146.2, more info at http://hamclub.org/

May 9 Dade City, East Pasco ARC Hamfest, Church Ave Overflow parking lot, 37746 Church Avenue, Talk-In on 146.880 -146.2, for info Chris Bloxsom , AA4CB, 224-221-5064 or aa4cb@arrl.net, nothing found on website.

May 23 **WormFest 2020, Pinellas Park, admission FREE, tailgate free, Freedom Lake Park, 9990 46th St N, southeast corner of US 19 and 49th Street, 33782. Park opens at sunrise for vendor setup, hamfest starts at 0800. Talk-in on 442.625 + or 146.850 – both with a tone of 146.2. For a map and directions see** http://www.TheWormholeSociety.org **.**

June 13 Dade City, Pre-ARRL Field Day Tail-Gators' Gathering, Dade City Masonic Lodge, 13642 21st St So, for info contact Gary Mentro , N3OS, 813-713-9994 or n3os@arrl.net

August 22 **TARCFest** TARC Clubhouse, 22nd St at the river, $5 entry including tailgate, a few inside tables reserved in advance, talkin on 147.105 +146.2, more info at http://hamclub.org/

November 14 Pinellas Park, **SPARCFest**, admission FREE, tailgate free, Freedom Lake Park, 9990 46th St N, Southeast corner of US 19 and 49th Street, Talk-in on 147.060+ no tone. VE testing at 0900. For more information go to https://www.sparc-club.org/sparcfest/

December 11 & 12 **Plant City, the 2018 Tampa Bay Hamfest is the Florida State Convention** and **West Central Florida Section Convention, Friday and Saturday, at the Expo Building in the Strawberry Festival grounds, advanced admission $9, at the door $10, for information contact Bill Williams AG4QX,** chairman@fgcarc.org **or go to** http://www.tampabayhamfest.org **or you can just ask me, Jim or Dee at a meeting ;-)**

Mid January	Adventure Run, Honeymoon Island
Last full weekend January	Winter Field Day, https://www.winterfieldday.com/
Late January	Gasparilla celebration
Late February	West Central Florida Tech Conference http://arrlwcf.org/wcf-special-events/wcftechconference/
Late February	MS 150 Citrus Tour bike ride http://www.citrustour.org/register.php
March/April	MS Walks
March/April	Mass Casualty Exercises
Late April	Southeastern VHF Society Conference, http://www.svhfs.org
Late April	Florida QSO Party
Mid May	March For Babies (was March of Dimes) https://www.marchforbabies.org/Registration/Events
Mid-May	Annual Armed Forces Crossband Test
Mid-May	Florida Hurricane Exercise
May, Memorial Day Weekend	Wormfest
Early June	Museum Ships on the Air
Fourth weekend in June	Field Day http://www.arrl.org/contests/announcements/fd/
July 3/4	Midnight Run in Largo http://www.kiwanismidnightrun.com/
August	International Lighthouse/Lightship Week https://illw.net/
October, 3rd weekend	JOTA, Scout Jamboree-on-the-AIR (around 14.280MHz)
Early December	ALS bike ride in Walsingham Park
December, Second weekend	Tampa Bay Hamfest http://www.fgcarc.org/

YOUR WORMHOLE OFFICERS

Bill AG4QX is President and editor of this newsletter, Treasurer is Jim KD4MZL, Paul KA4IOX is the Secretary, Dee N4GD is the Repeater Trustee and Mike K4ZPE is both our club Vice President and webmaster.

YOUR WORMHOLE REPEATERS

53.150 –1Mz PL 146.2

442.625 +5Mz PL 146.2

146.850 - 600Kz PL 146.2

The Wormhole repeaters are both now dual mode Yaesu DR-1X. FM analog as always and now Yaesu Fusion, a C4FM/FM digital mode.

The Wormhole website is at: http://www.TheWormholeSociety.org.

West Central Florida Section website: http://www.arrlwcf.org/.

The ARRL website is at: http://www.arrl.org/

This newsletter is written for The Glorious Society of the Wormhole, an ARRL affiliated amateur radio club located around the Seminole section of Pinellas County Florida. Anyone wishing to be added or removed from The Glorious Society of the Wormhole mailings please write to me at the address below and thy will be done.

73,
Bill Williams
AG4QX
ag4qx AT arrl DOT net