SWCP Portal
July 2017

Be alert, be careful, and above all, be backed-up

From Ransomware to Cyberwar

Another day, another threat, it seems. However, the latest alarm going out is nothing to yawn at. This attack has rapidly struck all around the world, rendering entire networks useless. Even worse, it leaves victims – including those who would pay the ransom demand – with little hope of ever recovering their files.

Petya is one name given to this latest nasty bit of malware. It encrypts victims' files, rendering them unusable, and can spread itself throughout corporate networks. All it takes is a single user in the local network to fall for a booby-trapped email to compromise the entire system.

As of this writing, Petya and related worms have struck multiple nations, starting in **Ukraine**. Everything from a part of **FedEx** to Danish shipping giant **Maersk**, a Tasmanian factory that makes **Cadbury chocolates**, and even Russian energy company **Rosneft** have **all** been hit.

In this country, drug firm **Merk**, at least one **nuclear plant** and the maker of Oreos have been hit. More big institutions have been taken down around the globe than ever before. They include the huge **port of Mumbai**, India, the world's biggest ad firm, **WPP,** plus the property arm of the largest French bank, **BNP Paribas**.

In Ukraine, **Petya** has struck their central bank, a metro system, airport, and power grid, even the Chernobyl **radiation monitoring system**. At least 80 other Russian and Ukraine **companies** have also been struck.

Worse than ransomware

If this somehow sounds familiar, it's because this assault follows hard on the heels of a similar institution-crippling ransomware virus, **WannaCry** which struck numerous hospitals in Britain.

Like WannaCry, Petya uses several NSA exploits stolen by the mysterious **Shadow Brokers** group. These were integrated months ago with three off-the-shelf hacking tools. First spread by targeted spearphishing emails, once established in a networked computer, this worm can spread itself stealthily throughout entire computer networks, which makes it particularly dangerous .

Unlike WannaCry, no convenient built-in **killswitch** has yet been found to thwart attacks. However, researchers have located a way to **vaccinate** computers, albeit temporarily, by changing a single local filename.

The hackers demand payment in Bitcoin, generally from $300 to $500, to restore the device. However, this won't work for Petya. For one thing, the email address to which victims are to reply has been disabled by the provider.

Moreover, the latest version, called **NotPetya** by the **Kaspersky Lab**, the Russian security firm that analyzed it, is *not* designed to allow unencryption of bricked machines. It is simply intended to **destroy systems**. The ransomware demand is thought to be a ruse to disguise its true intent and origin and confuse victims. It is believed to have started when an **autoupdate server** for MeDocs, a Ukrainian tax accounting software provider, was compromised in June.

While WannaCry was suspected to be Russian or North Korean, Petya and especially NotPetya are

thus likely to be a **Russian cyberweapon** aimed at Ukraine, with a lot of collateral damage. **This may be what cyberwar looks like**. As long as their targets are successfully hit, such state hackers don't care what else goes down.

Even more than such attacks hitting unintended targets, the most disturbing things about these are their use of sophisticated NSA exploits, stockpiled and paid for by the American taxpayer. Angry victims and tech companies are **demanding** some security for ordinary users, while the National Security Agency remains silent and the government blames it all on foreign adversaries.

Protecting your precious files

Once informed by the NSA, Microsoft rolled out patches in March and later issued an emergency one for older Windows systems in May. But there are at least *38 million* PCs worldwide still unpatched, **according** to Avast cybersecurity.

However, the attack requires local adminstrative rights to deliver the payload. For most users, setting up a standard account on their machine for regular use can help avoid such compromises.

Yet, even this may not prevent infection, especially if your machine is a part of a large corporate network. Your first warning could be when your computer suddenly tries to reboot. It may be possible to halt the infection by turning it off at that point. So another **method** is to disable Windows' ability to automatically reboot after crashing. But it is much better, of course, to do whatever possible to avoid infection and to be prepared in case the worst actually happens.

Users really can't be too suspicious about email these days. No longer are spam emails easily detected by poor spelling and strange text inclusions. **Spearphishing emails** have become extremely sophisticated these days, carefully crafted to be indistinguishable from legitimate messages from bosses and trusted institutions.

There may be a few telling details that can give the game away. First of all, check the **actual reply address**. While the senders' name can be easily spoofed, the email address (which appears within angle brackets like <help@swcp.com>) cannot be. Depending on your email client, seeing the real address is not always automatic, but most can be configured to do so. See our blog post for more information and instructions

Hackers *must* use domains under their own control, so either the link will go to a different domain entirely than the one the institution normally uses, or a look-alike. **Check for hyphens and subtle variations** on the name of the place, or the use of a different top-level domain (such as "amazon.biz" rather than "amazon.com".)

Don't be pressured into an panicked response. Remember that law enforcement agencies, the IRS, and financial institutions, for instance, *never* use email to demand account information or threaten people with fines or lawsuits. And don't be shy about forwarding any suspicious-looking emails to be checked out by SWCP's Tech Support at ***help@swcp.com***. (In fact, you'll be helping keep all the rest of us safe if you do.)

It's best not to click on links in emails. Trap sites often use the domain disguising techniques mentioned above. But even if they appear absolutely legit, it's best to visit the institution's website from a bookmark or Google the address.

But you can do everything right and still get slammed. Thus, the only sure way to keep your files secure from all such threats as will inevitably arise is to constantly **back up your files**.

There are **various ways** of doing this – see our **white paper** for a helpful overview. Most methods, however, require some discipline to do consistently. Possibly the easiest method is the **SWCP BUS** online backup system. Starting at just $10/month (plus discounts for users of our broadband services) the BUS is an automatic and worry-free method that keeps updated files available for instant downloading as needed.

It doesn't matter *how* you back up your system, just that you do it regularly. For life is largely online these days, and few things are more devastating than suddenly losing large pieces of it.

Archived at: http://www.swcp.com/newsletters/.
Click on blue terms in PDF file to open links.