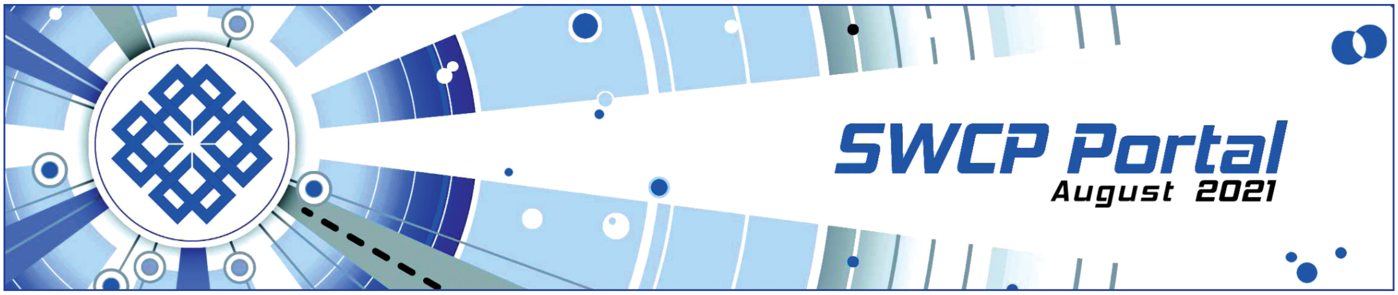

SWCP Portal
August 2021

Malware Madness

Even as the coronavirus wreaks havoc across the planet, a similar pandemic plague of sorts is causing chaos throughout cyberspace. **Malware**, malicious software of all kinds, is silently spreading through systems both large and small, seeking to infect and take over or destroy any device open to contagion.

Like Covid, although much more diverse, malware has disrupted society in our attempts to fight it. Losses to the economy are staggering – malware may **cost** *$6 trillion* this year alone, expenses soaring with each attack. In cyberspace there are firewalls instead of masks, data limiting and other schemes to keep others distant, but alas, no vaccines.

Not to strain that analogy, but the situation could also be seen as a vicious street fight in a dark alley of all against all. For by any measure the situation is out of control and growing worse by the day.

The lure of cybercrime

There are several reasons why **ransomware**, **phishing** and other scams are going wild right now. The first reason is the pandemic itself. Covid made internet access absolutely vital while at the same time forcing millions to stay at home without the protections of the company IT space. Workers setting up home offices on their own had to try new things.

People were online more of the time, too, working, shopping, banking, and just hanging out. They were more accessible, vulnerable, and highly reliant on the net, which made them very tempting targets.

Cybercrime does pay, and often handsomely, too. Probably the biggest hit was the ransomware attack over the Fourth of July weekend by Russian-linked hackers **REvil** of 1,000 or more IT organizations in 17 countries. They **demanded** *$70 million* to release a decryption tool, or *$45,000-$5 million* from individual firms. It's not known how much they got as they completely **disappeared** a week later.

Another reason crime online flourishes is that low-end methods are so much more available and easy for homegrown hackers now while the high-end methods are constantly becoming more sophisticated. In **dark web forums**, personal data from mass data breaches may be sold in bulk, and others where criminals could purchase off the shelf malware packages to go, no programming expertise needed.

At the top end are attacks like that devised by REvil. The way they were able to infect so many computer systems is that they somehow successfully hid their ransomware bomb in a **supply chain attack**.

The **biggest known** such assault so far was the **SolarWinds** operation discovered in late December by a security firm among those hacked. Executed by **CozyBear**, the Russian hackers responsible for penetrating the Democratic National Committee (and **more recently**, the Republicans), they inserted their malware inside updates to install a **backdoor** into a network monitoring platform. Microsoft Office 365 was also apparently used to spread the virus.

18,000 servers, including those of the Pentagon and other agencies along with Fortune 500 companies, were infected but only *40* or so got additional malware packages, indicating this was more espionage of carefully-chosen targets than anything else.

In the **Kaseya attack**, REvil exploited a previously unknown vulnerability in that brand of servers sold to other firms. Kaseya later acquired the **decryptor** software from a third party and quickly restored files while hardening their own internal security.

Another cunning scheme just exposed involves fake sites virtually identical to real ones complete with valid security certificates. Domains of these sites rely on a little-known feature called **punycodes**, a formulaic way to insert accented letters in domain names. In one case, hackers fooled users seeking a free browser from "brave.com" for a domain that appears as "bravé.com" (note the accent over "e") where they would instead get **malware** allowing hackers to spy on their desktops or their internet connections.

The gathering storm

Perhaps the most disturbing trend fueling the rise of cybercrime is the convergence between criminal activities for monetary gain with state-sponsored hacking for intelligence-gathering, blackmail, and sabotage of vital industries and services. Nowadays victims could, and some have, had all their secrets stolen, resold, or released on the internet to embarrass them, partners and contacts compromised, and their internal data stolen, held for ransom and/or destroyed, with malware penetrating so deeply into their systems that all the hardware must be replaced.

Spies have partnered with criminals on unsavory projects for a very long time, but it has always been hard to obtain real proof, especially in online cases. Secrecy and lies are their stock in trade, after all.

Another major attack that could be both cybercrime and warfare occurred in early May. **Colonial Pipeline** was completely turned off by a ransomware assault that halted vital petroleum supplies to the East Coast, leading to long lines and gas shortages. In desperation, the CEO paid the *$11 million* ransom over the protests of the FBI.

But **Darkside** – the group behind the attack – also disappeared after the payout just like REvil did. Both are believed to be comfortably situated in Russia, where they have inconvenienced no one at all.

The timing of this vanishing act, coming right after their demands were met, is quite suspicious. For at the same time in early July, President Joe Biden threatened Putin with "consequences" in a **phone call**, though the former-KGB spy **dismissed** the threats as "farcical" based on "unfounded accusations", demanding proof of Russian involvement.

But to offer *any* kind of proof would expose not only what the US knows but how it was obtained. Plus, any retaliatory hacks could lead to serious escalation. In both **2015** and **2016** Russia took down Ukraine's power grid in the dead of winter. It is quite likely that our grid has also been mined with malware agents and we've probably done the same to Russia. It's a brand-new Cold War; and any mistake – especially in attributing attacks – could be deadly.

However, Russia just **submitted** a draft convention on fighting cybercrime the UN General Assembly. The hacking hotbed proposed a broad extension to current rules, outlawing **deepfakes** but also wanting backdoors to systems provided to authorities.

It will be quite interesting to see how this develops. A general treaty to fight cybercrime would have to have more teeth than the **Paris agreement** to combat climate change. But just outlawing criminal hackers any safe havens could be a good start.

Doing your bit to stay safe online

In the meantime, what can the average user do to safeguard their data? As with Covid, it would seem like not much. But many infections are due to personal lapses of protection. Discipline is required.

- Do not click on *any* email address links in emails – they could be spoofed. Likewise, do not google help or customer service numbers and email, but use *only* those provided on official websites.
- Back up *everything* on a regular schedule. Either copy it to a thumb drive or removable HD nightly or subscribe to a reliable online backup service like **SWCP BUS** that is automatic and secure.
- Use antivirus clients on all your devices – Macs as well as PCs. Commercial services are cheap and far less prone to harbor spyware than freebies.
- Set your privacy protections on those devices (especially smartphones) to the highest setting that doesn't interfere with actual use.
- *80%* of malware attacks are delivered by phishing, so your first line of defense is constant attention. Note addresses and spelling carefully.

If you see something suspicious, notify SWCP Tech Support to have it checked. Remember, we're all together in *this* pandemic, too. Stay safe, be vigilant!

Phone Numbers Are Getting Longer

By Mark Costlow, SWCP President

As of April 24 of this year, New Mexico entered a "**permissive dialing**" period, which means that we can now make all calls with **10-digit numbers**. But beginning **October 24, 2021**, 10-digit dialing will be mandatory. If you try to dial with only 7 digits, you'll get a frustrating "hang up and try again" message.

Why the change? A new 9xx number, 988, was recently assigned to the National Suicide Prevention Lifeline. Since "988" is already a valid phone number prefix here in New Mexico, any time you tried to call someone with a 988-xxxx number, you would get the country-wide Suicide Hotline instead, which could be rather embarrassing, to say the least.

With 10-digit dialing, here in the Albuquerque area, you'll dial 505-988-xxxx to reach that friend or business, and the phone system will know that's what you want and you're not actually so fed up with telephones that you're thinking of ending it all.

Things to check before October:

- If you use **dialup** internet (there are still a few of you still out there), make sure your modem dialing software is set to call a full 10-digit number.
- If you have an **office** phone system, contact the vendor to check that it is already using 10-digits, or have it updated to do so. It is usually a simple change. Ironically, on an office PBX you might still be able to dial 7 digits as the PBX usually automatically converts that to 10-digit dialing for you, but you need to be sure the PBX is ready.
- Remember that *all* calls made to anywhere in the US or Canada outside your area code, including toll-free 800 numbers, require **dialing "1" first**.

Southwest Cyberport

New Mexico's Expert Internet Service Provider since 1994

505-232-7992 | *swcp.com* | *Tech support:* ***help@swcp.com***
5021 Indian School NE, Ste. 600, Albuquerque, NM 87110

Please click on ***bold blue type*** *in text for links to sources.*