The Malware Free for All
Or, Put Me In Coach, I'm Ready To Play

Well, there's fist fights in the kitchen, they're enough to make me cry
Then the milkman comes in, even he's gotta take a side
— On the Road Again, Bob Dylan

The much vaunted cyberwar has come to resemble less a war than a benches clearing brawl at a ballgame. Every player on every team has come out to throw a punch. And get punched back in the ensuing melee. A survey of companies around the globe made by **security vendor Proofpoint** reported that, "**83% of survey respondents revealing their organization experienced at least one successful email-based phishing attack, up from 57% in 2020**." This past year saw a "**46% increase in organizations hit with a successful phishing attack last year**." The country from where the greatest phishing attacks emanated was the US, **"accounting for 73% of internet service providers hosting these types of attacks**." The same report showed that the USA is both the Number 1 Perp and also the Number 1 Vict when it comes to email phishing attacks. **Huzzahs! Score one for the home team!**

One doesn't usually think of Germany as the originating hotbed of cyber criminality. Nevertheless, that seems to be where **TeamTNT hails from**. "**The majority of their tweets are written in German and the account's location is set to Germany. In addition, many comments in the shell scripts used by the threat actor are written in German. Therefore, it can be assumed that TeamTNT's country of origin is Germany**."

Hacker groups, such as TeamTNT, are not really determined to bring down Western Civilization, but simply out to make a dishonest buck by placing **LemonDuck malware on Amazon Web Services servers for the purpose of cryptomining**. A TrendMicro special report on TeamTNT described their motivations thusly: "**The actors behind TeamTNT profile themselves either as "honest robbers" who mean no harm or as red team penetration testers, often teasing security researchers in the process**." **[ed. A PDF will open.]** The report noted that, although the actions of TeamTNT might not cause physical harm to its victims, "**the group's seemingly "harmless" activity can actually cause heavy financial losses**."

"**Known to strike both Windows and Linux environments**," LemonDuck is primarily engineered for abusing the system resources to mine the crypto currency, Monero. But it's also capable of **"credential theft, lateral movement, and facilitating the deployment of additional payloads for follow-on activities**." I.E., planting the seeds for future attacks. In July 2021, **Microsoft did an in-depth analysis of the LemonDuck malware**.

> **LemonDuck, an actively updated and robust malware that's primarily known for its botnet and cryptocurrency mining objectives, followed the same trajectory when it adopted more sophisticated behavior and escalated its operations. Today, beyond using resources for its traditional bot and mining activities, LemonDuck steals credentials, removes security controls, spreads via emails, moves laterally, and ultimately drops more tools for human-operated activity.**

An in-depth analysis of TeamTNT and their actions can be had **here** by German security firm, Intezer. Dated February 18, 2022, this is the most recent complete reporting, albeit somewhat technical.

It is not just large enterprises undergoing nonstop assault, so has the more consumer side of computing recently been victimized by miscreants' malware. Two popular and generally well received open-source applications, not exclusively, but widely adopted by Windows users, have recently been found to have been reversed engineered and had malware implanted into the

apps. "**7-Zip is a pretty old piece of open-source software. Its interface, buttons, and help menu haven't changed much since 1999,**" is how reviewgeek.com editor, Andrew Heinzman, described the file zip/unzip application 7-Zip. The charge here is that 7-Zip will open a user to privilege escalation. **Privilege escalation is best described as**:

> **Privilege escalation is a type of network attack used to gain unauthorized access to systems within a security perimeter. Attackers start by finding weak points in an organization's defenses and gaining access to a system. In many cases that first point of penetration will not grant attackers with the level of access or data they need. They will then attempt privilege escalation to gain more permissions or obtain access to additional, more sensitive systems.**

The **7-Zip situation is disputed**. Some researchers have not been able to repeat the privilege escalation. **The researchers who discovered the vulnerability stand by their work**. My own experience with 3rd party ZIP apps is that they too often come laden with adware and spyware, as do so many open source consumer related applications. **Besides, both Windows 10 and Windows 11 come with their own perfectly useable zip utilities. I do not understand why there is any need for Windows user to install a stand alone zip utility.**

On the other hand, one useful piece of software that DOES NOT come with either Windows 10 or Windows 11 is what is known as a codec for playing DVD movie disks on a computer. **Microsoft describes a codec this way**:

> **A codec compresses or decompresses media files such as songs or videos. Windows Media Player and other apps use codecs to play and create media files. A codec can consist of two parts: an encoder that compresses the media file (encoding) and a decoder that decompresses the file (decoding).**

And what Windows is missing is the the **DVD decoder.**

> **A DVD decoder is another name for an MPEG-2 decoder. The content on DVD-Video discs is encoded in the MPEG-2 format, as is the content in DVR-MS files (Microsoft Recorded TV Shows) and some AVI files. To play these items in the Player, you need to have a compatible DVD decoder installed on your computer. If your computer has a DVD drive, it probably already has a DVD decoder installed on it**

The article referenced is a wee bit out of date, however. Yes, in the days when computers came with optical drives, the PC also came with some bloated consumer media player application that took over all media handling by default, but did contain the DVD decoder software to play DVD movies on the PC. That was then; and this is now. PCs generally do not come with optical drives anymore. Thin and light being the order of the day.

Enter **VLC player**, an open source application for playing just about any type of media file, and especially DVD movie disks. It has been **incredibly well received by one and all within the digerati corps**. In fact, it is the only open source software that I have ever used myself or recommended and installed on clients' PCs — until two weeks ago. **Enter the Dragon**. Otherwise, known as **Cicada.**

This Chinese hacker group is well known by Western intelligence and law enforcement, having been around since 2006. "**The start of Cicada's current campaign has been tracked to mid-2021 and was still active in February 2022**."

On April 5, 2022, in an article that was widely cited by other respected sites, **BleepingComputer**, reported that:

> **Security researchers have uncovered a long-running malicious campaign from hackers associated with the Chinese government who are using VLC Media Player to launch a custom malware loader. The campaign appears to serve espionage purposes and has targeted various entities involved in government, legal, and religious activities, as well as non-governmental organizations (NGOs) on at least three continents.**

Effectively, what Cicada accomplished was to "side-load" an infected version of the VLC player to replace the legit player. "**The technique is known as DLL side-loading and it is widely used by threat actors to load malware into legitimate processes to hide the malicious activity**".

Microsoft offers a DVD codec player for $14.99 a year. (I believe it is a yearly subscription.) It is an incredibly well kept secret, however. Although the MS player does download from the Microsoft Store, searching the store for the player software will not help. **Click this link**. When the MS webpage loads, then click the **blue Get Windows DVD Player button.** This will open the Microsoft store page for the software. There is a free trial to test that the player will work on your configuration. It is only a test. **The free trial WILL NOT PLAY a movie**. FYI: It worked on my PC. It has worked for others. By installing the MS DVD Player, whatever is your current media playing software will not be affected, unlike those bloated consumer DVD player packages.

What these two situations point out is the **open source vs proprietary** software controversy and debate is longer only the purview of governments and large installations. Open source software is once again plaguing the Google Play Store. **PC Magazine reported** April 7, 2022, that "**Security researchers recently uncovered six fake antivirus apps on the Google Play Store that installed malware**." This malware had been "**downloaded over 15,000 times**," before Google removed the app.

Also discovered on the Google Play Store was the Octo malware. The Octo malware hides on the victim's phone and intercepts and scoops up just about everything that happens on the phone. **It is generally believed that this new strain of Android malware is a repurposed attacker from 2016**, with its origins in Russia.

> **In mid-2021, a new Android banking malware strain was spotted in the wild. While some AV companies dubbed it as a new family with the name "Coper", ThreatFabric threat intelligence pointed towards it being a direct descendant of the quite well-known malware family Exobot. First observsed in 2016, and based on the source code of the banking Trojan Marcher, Exobot was maintained until 2018 targeting financial institutions with a variety of campaigns focused on Turkey, France and Germany as well as Australia, Thailand and Japan. Subsequently, a "lite" version of it was introduced, named ExobotCompact by its author, the threat actor known as "android" on dark-web forums.**

Octo was spread by several Play Store apps, most notably "**an app named "Fast Cleaner**," which had 50,000 installs until February 2022, when it was discovered and removed. **I can only wonder how many of those 50,000 infected phones will be used in the next attack on a water treatment plant somewhere in the US? That's the way the Internet works.**

What these and so many other incidents point out is the open source vs proprietary software debate is no longer theoretical. **Open source: think Log4j debacle involving Java vulnerabilities. Proprietary software: think Microsoft and Apple.**

Open source software has been weaponized to fight in the real war. **An open source developer in Ukraine modified open source software to make a statement to Russians about the war**. Another open source developer corrupted a common open source Javascript, **Npm**, to protest the war. **But it took a sinister turn along the way.**

> **It started as an innocent protest. Npm, JavaScript's package manager maintainer RIAEvangelist, Brandon Nozaki Miller, wrote and published an open-code npm source-code package called peacenotwar. It did little except add a protest message against Russia's invasion of Ukraine. But then, it took a darker turn: It began destroying computers' file systems.**
>
> **To be exact, Miller added code that would delete the file system of any computer with a Russian or Belorussian IP address. Then, its maintainer added the module as a dependency to the extremely popular node-ipc mode. Node-ipc, in turn, is a popular dependency that many JavaScript programmers use. And it went from annoying to a system destroyer.**
>
> **The code has undergone several changes since it first appeared, but it must be regarded as highly dangerous. Underlining its potential for damage, Miller**

> **encoded his code changes in base-64 to make it harder to spot the problem by simply reading the code.**

One might be so inclined to root these actors on with a hearty **HUZZAH**. They seem to be playing for the home team and are on the right side of ***European History.*** But to cheer them on is to ignore how the Internet works. **There is no boundary to the network is a first principle of Zero Trust**. **It is more than simply the logic of Karma to state that on the Internet "What goes around, comes around." It is, in fact, the most simple explanation for how malware spreads.**

In August 19, 2019, an article appeared in securitytoday.com entitled ***The Dangers of Open-Source Vulnerabilities, and What You Can Do About It.*** The article states succinctly the trade-offs enterprises make when they develop their applications with open source software. **"Currently, about 96 percent of the applications in the enterprise market use open-source software. On the one hand, this makes development easier for both developers and third-party vendors. On the other hand, it presents risks and exposes some die-hard vulnerabilities."**

The article rightfully states that both open source and proprietary suffer from the same imperfections. Noting that open source and proprietary software both "**involve poorly written code, leaving "holes" or gaps that attackers can use to carry out malicious activities, such as modifying the code to extract sensitive data or damage the system**." What sets open source software apart from proprietary software is a "**dedicated staff of professional developers is behind proprietary software, writing the code according to the directives of their organization. On the other hand, open-source is, well, "open," meaning anybody can write, fix and maintain the projects**." Think Microsoft's Patch Tuesday on the one hand, and the near crisis patching open source has been of late. On April 21, 2022, it was reported that "**Amazon's Hotpatch for Log4j Flaw Found Vulnerable to Privilege Escalation Bug**." The Log4j crisis started in December 2021, but is still very much present and wreaking havoc because operators have not patched, or their patches failed.

The most egregious example of valuable open source software that is now corrupted is the example of SNORT. Snort is now maintained by Cisco, and is a very popular and well established intrusion detection application that has been in service by security professionals for years, including yours truly at one time long ago. Cisco noted that: "**A successful exploit could allow the attacker to cause the Snort process to hang, causing traffic inspection to stop**." With the ultimate result in hackers taking over the network via the software designed to root the attackers out.

> **In other words, exploitation of the issue could allow an unauthenticated, remote attacker to create a denial-of-service (DoS) condition on affected devices, effectively hindering Snort's ability to detect attacks and making it possible to run malicious packets on the network.**
>
> **"Successful exploits of vulnerabilities in network analysis tools such as Snort can have devastating impacts on enterprise and OT networks."**

Of course, now the stakes are far higher when software has been found to be corrupted. If Russian hackers can wipe Ukrainian hard drives and/or vice versa, then any hacker from anywhere can wipe your root drive, and my root drive, and just about anyone else's drive. I have maintained for many years that eventually the computer and the network will have to be managed and maintained by a partnership between governments and private businesses. Much like utilities are today.

And to this end, **Microsoft just might do away with Patch Tuesday** because people are just too ignorant, too lazy, or just plain too stupid to patch their software. At least, that's my take on it. Read on.

Oh, put me in coach, I'm ready to play today
— Centerfield, John Fogerty

Back to Top

Gerald Reiff

Back to Top

next post →