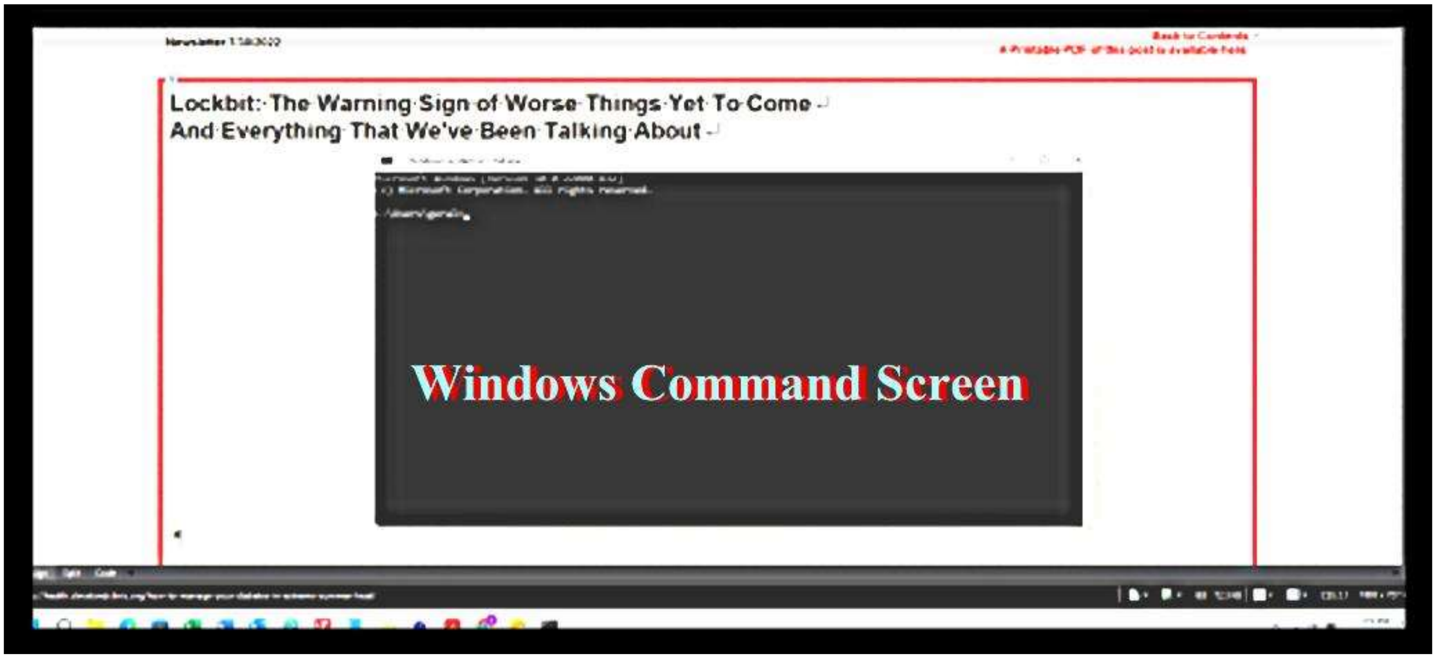
Top

Newsletter 7/30/2022

Back to Contents
A Printable PDF of this post is available here.

Cobalt Strike: The Warning Sign of Worse Things Yet To Come
And Everything That We've Been Talking About



Newsletter 7/30/2022

Back to Contents
A Printable PDF of this post is available here.

Lockbit: The Warning Sign of Worse Things Yet To Come
And Everything That We've Been Talking About

```
Microsoft Windows [Version [illegible]]
(c) Microsoft Corporation. All rights reserved.

C:\Users\gerald>
```

A Windows Command Prompt Screen

On July 28, 2022, "**Cybersecurity research company SentinelOne**," published news that quickly spread among the digerati. The Microsoft antimalware application, Windows Defender, had become compromised. More specifically, the Windows Defender Command Line tool had fallen victim to a sideloading scheme that has the Command Line Tool "**being abused to load Cobalt Strike beacon on to potential victims,"** **neowin.net reported it, July 29, 2022**. And then, in turn, as **BleepingComputer reported, July 29, 2022**, that vulnerability is currently exploited to infect victim computers with LockBit ransomware.

What I must emphasize, but cannot yet say with complete confidence about the validity of the statement, that it is only the Command Line Tool component in Windows Defender that has been reported to be compromised. Many users would not have any reason to run the Command Line Tool. As the **Microsoft posting of May 13, 2022**, that explains how and why to use the Command Line Tool, states:

> **You can perform various functions in Microsoft Defender Antivirus using the dedicated command-line tool mpcmdrun.exe. This utility is useful when you want to automate Microsoft Defender Antivirus tasks. You can find the utility in %ProgramFiles%\Windows Defender\MpCmdRun.exe. Run it from a command prompt.**

So, for instance, if a network administrator wanted to enable automatic malware scanning of desktops on the network, she might configure that task using the tool.

The actions that initiated the compromise itself happened months ago. As SentinelOne researchers found, "**The initial target compromise happened via the Log4j vulnerability against an unpatched VMWare Horizon Server**." Readers may remember the near panic security researchers and experts were in around New Years. The Log4j logging app was used in many different applications and device interfaces, and then went weeks without effective patching.

One constant comment this reporter often makes when cyber security incidents are reported goes like this: "**We may know what the crooks stole; but do we know what they left behind?**" SentinelOne researchers laid out the steps the hackers took to achieve their ends.

> **1. Once the attackers gained initial access via the Log4j vulnerability, reconnaissance began...**
> **2. Once the threat actor acquired sufficient privileges, they attempted to download and execute multiple post-exploitation payloads.**
> **3. The threat actor downloads a malicious DLL, the encrypted payload and the legitimate tool from their**

> **controlled C2 (Command and Control server):**
> **4. Notably, the threat actor leverages the legitimate Windows Defender command line tool MpCmdRun.exe to decrypt and load Cobalt Strike payloads.**

Cobalt Strike itself is **"a legitimate penetration testing suite with extensive features popular among threat actors to perform stealthy network reconnaissance and lateral movement before stealing data and encrypting it,"** according to **BleepingComputer, ibid.** Any tool of any kind can be beneficial or destructive, depending who wields the tool and why.

This attack and similar attacks facilitated by backdoors left behind by heretofore known or unknown attackers is why any attack on one network resource should be considered an attack on all network resources. The notion that **The Network Has No Boundary** is a primary tenet of Zero Trust, at least as I interpret the framework. Simply put, computer security incidents do not take place in a vacuum. The attack on Windows Defender discussed herein is just one of the many security incidents that have arisen due to the continued fallout from the Log4j debacle. It must be remembered that Loj4j **"is likely present in hundreds of millions of devices**," as explained in a report by **ZDNet, Dec. 14, 2021,** and as the Log4j attacks were in full swing. **Seven months later, The Cyber Safety Review Board (CSRB), established to investigate and have a federal response to major cyber incidents, concluded that:**

> **Most importantly, however, the Log4j event is not over. The Board assesses that Log4j is an “endemic vulnerability” and that vulnerable instances of Log4j will remain in systems for many years to come, perhaps a decade or longer. Significant risk remains.**

Despite all the in-depth reporting surrounding Log4j, and the universal clarion call to patch and patch again, the CSRB concluded in July 2022 that: "**organizations still struggled to respond to the event, and the hard work of upgrading vulnerable software is far from complete across many organizations**." **Download the complete CSRB report in PDF here**.

So, we can expect more incidents like the one described herein concerning Windows Defender and other legitimate applications. We can also expect more legitimate and illegitimate sideloading of applications. The difference between a legitimate application and a sideloaded application was explained in **CSO, Dec. 2, 2021**.

> "**The key difference between sideloading and a normal installation is that in sideloading, the application has not been approved by the developer of the device’s operating system.**”

It is the ease in which hackers can inject malware into the otherwise legitimate applications that has Google, and Apple in particular, very anxious about the "**Open App Markets Act, a bill that targets dominant app stores**." As **Apple contends**, and all evidence shows:

> **...enabling sideloading would result in a flood of new attacks on iPhone users from bad actors eager to access the sensitive data stored on consumer devices. Predators and scammers would be able to "side-step Apple's privacy and security protections completely," with the bill allowing "malware, scams, and data-exploitation to proliferate.**

Finally, to my dear readers, who may now doubt the confidence that this blogger and others have placed in Windows Defender, my advice is to ensure that your installation of Windows Defender is the most current version available. That's the topic of the next post.

Now everything is upside down
Everything has got a shade of blue
I don't know if it's something that'll pass away
Or something that I gotta get used to
— Everything Upside Down, Mike McClure

Gerald Reiff

Back to Top **← previous post** **next post ⟶**