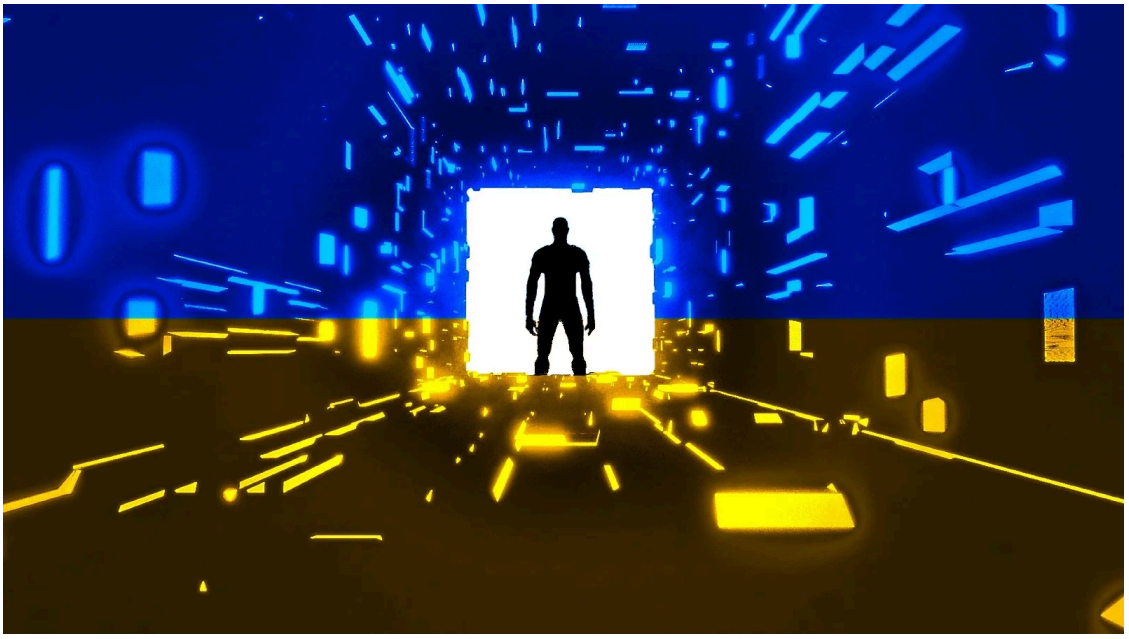
The Week in Ransomware - April 1st 2022 - 'I can fight with a keyboard'

By Lawrence Abrams

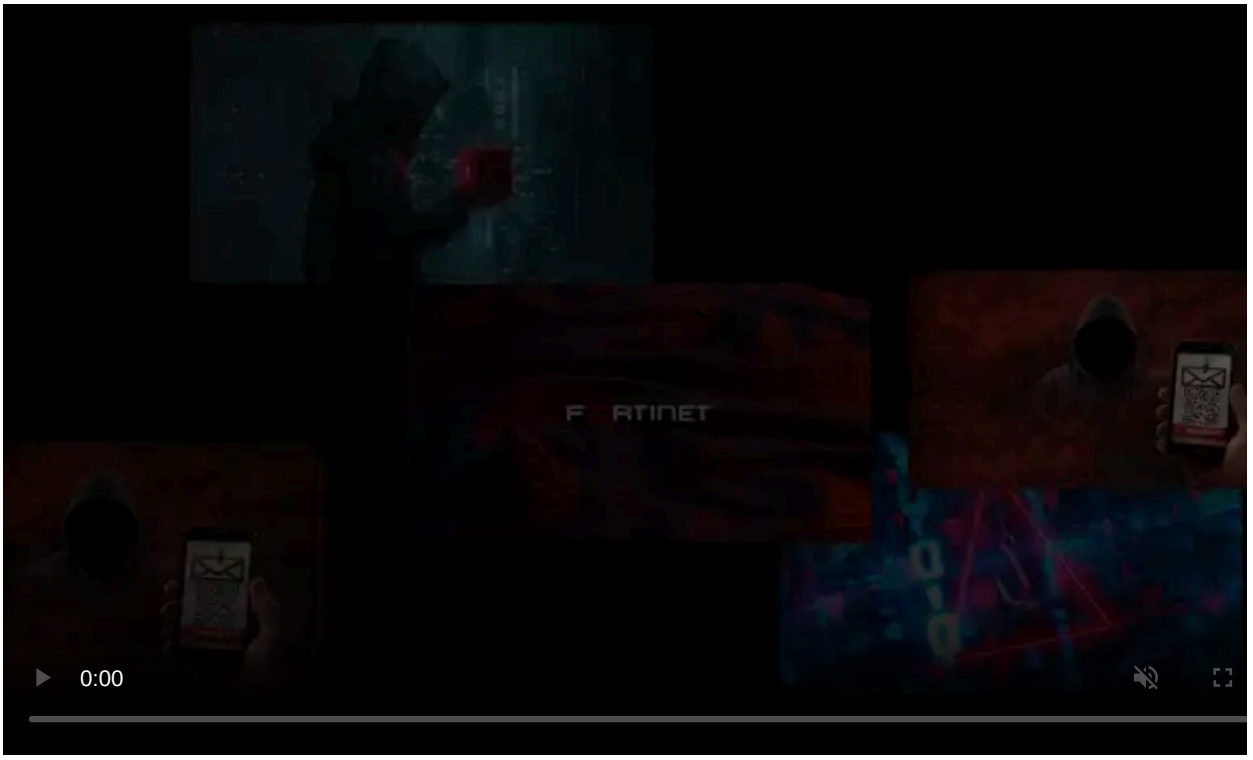
Published: 2022-04-01 · Archived: 2026-04-05 23:07:40 UTC

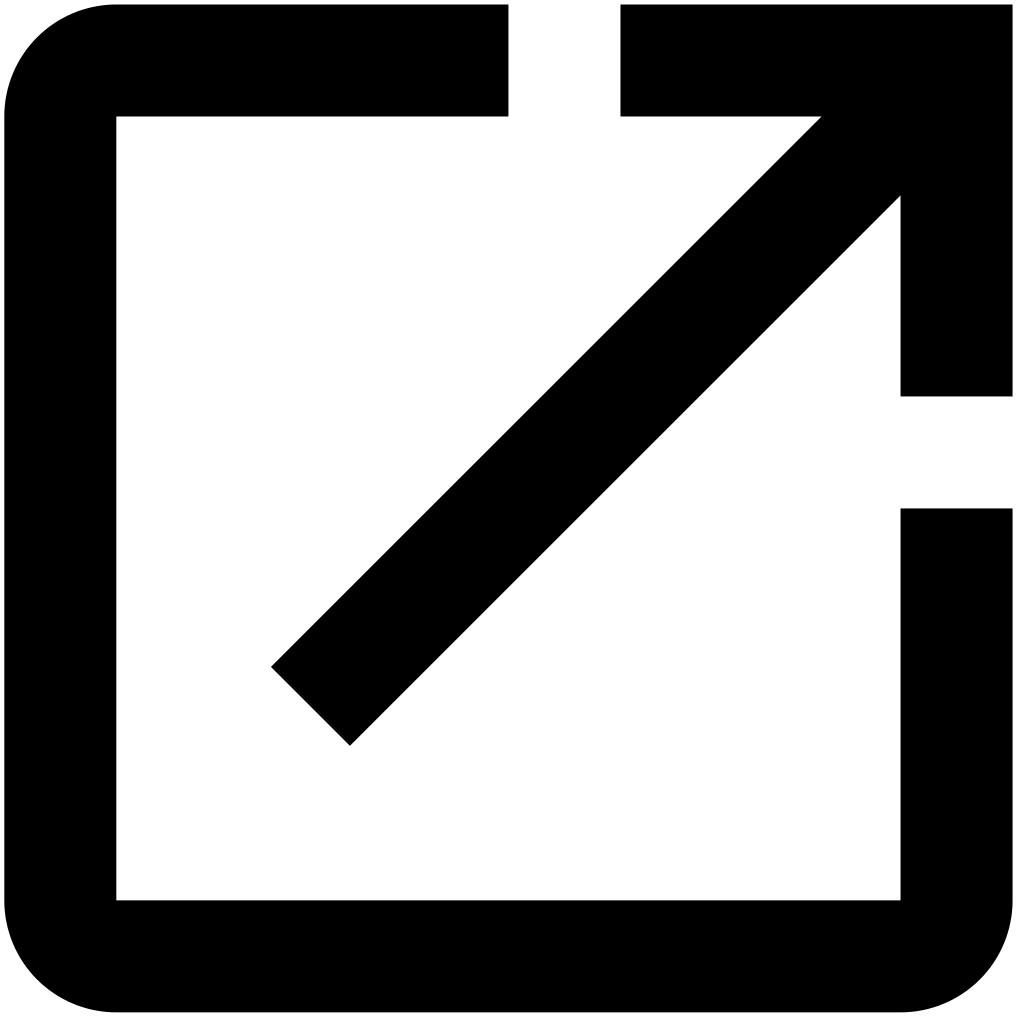


While ransomware is still conducting attacks and all companies must stay alert, ransomware news has been relatively slow this week. However, there were still some interesting stories that we outline below.

This week's most interesting story is CNN's report on Conti Leaks, a Ukrainian researcher who has had access to Conti's internal servers for years.

After Conti sided with Russia over the invasion of Ukraine, the researcher fought back by leaking internal chats and source code for the Conti Ransomware gang, providing researchers and law enforcement a glimpse into their operations.


F RTINET
0:00



Other interesting news is a clever 'IPFuscation' technique used by the Hive ransomware gang to obfuscate payloads by representing them as IP addresses to evade detection. By running the list of IP addresses through a decoder, it results in a binary payload that can be installed.

Contributors and those who provided new ransomware information and stories this week include: @PolarToffee, @FourOctets, @jorntvdw, @LawrenceAbrams, @Seifreed, @serghei, @malwrhunterteam, @DanielGallagher, @VK_Intel, @malwareforme, @Ionut_Ilascu, @struppigel, @demonslay335, @fwosar, @billtoulas, @BleepinComputer, @rivitna2, @MinervaLabs, @Amigo_A_, @SentinelOne, @AquaSecTeam, @ContiLeaks, @snlyngaas, and @pcrisk.

March 27th 2022

Hive ransomware ports its Linux VMware ESXi encryptor to Rust

The Hive ransomware operation has converted their VMware ESXi Linux encryptor to the Rust programming language and added new features to make it harder for security researchers to snoop on victim's ransom negotiations.

March 28th 2022

SunCrypt ransomware is still alive and kicking in 2022

SunCrypt, a ransomware as service (RaaS) operation that reached prominence in mid-2020, is reportedly still active, even if barely, as its operators continue to work on giving its strain new capabilities.

New KalajaTomorr ransomware

Amigo-A found a new ransomware that drops a ransom note named **Hello.txt**.

March 29th 2022

Threat Alert: First Python Ransomware Attack Targeting Jupyter Notebooks

Team Nautilus has uncovered a Python-based ransomware attack that, for the first time, was targeting Jupyter Notebook, a popular tool used by data practitioners. The attackers gained initial access via misconfigured environments, then ran a ransomware script that encrypts every file on a given path on the server and deletes itself after execution to conceal the attack. Since Jupyter notebooks are used to analyze data and build data models, this attack can lead to significant damage to organizations if these environments aren't properly backed up.

New Dharma ransomware variant

PCrisk found a new Dharma ransomware variant that appends the **.snwd** extension.

March 30th 2022

Hive ransomware uses new 'IPfuscation' trick to hide payload

Threat analysts have discovered a new obfuscation technique used by the Hive ransomware gang, which involves IPv4 addresses and a series of conversions that eventually lead to downloading a Cobalt Strike beacon.

'I can fight with a keyboard': How one Ukrainian IT specialist exposed a notorious Russian ransomware gang

As Russian artillery began raining down on his homeland last month, one Ukrainian computer researcher decided to fight back the best way he knew how -- by sabotaging one of the most formidable ransomware gangs in Russia.

March 31st 2022

LockBit victim estimates cost of ransomware attack to be $42 million

Atento, a provider of customer relationship management (CRM) services, has published its 2021 financial performance results, which show a massive impact of $42.1 million due to a ransomware attack the firm suffered in October last year.

Four new STOP ransomware variants

PCrisk found new STOP ransomware variants that append the **.voom**, **.mpag**, **.gtys**, or **.udla** extensions.

That's it for this week! Hope everyone has a nice weekend!

Source: https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-1st-2022-i-can-fight-with-a-keyboard/