The Week in Ransomware - November 13th 2020 - Extortion gone wild

By Lawrence Abrams

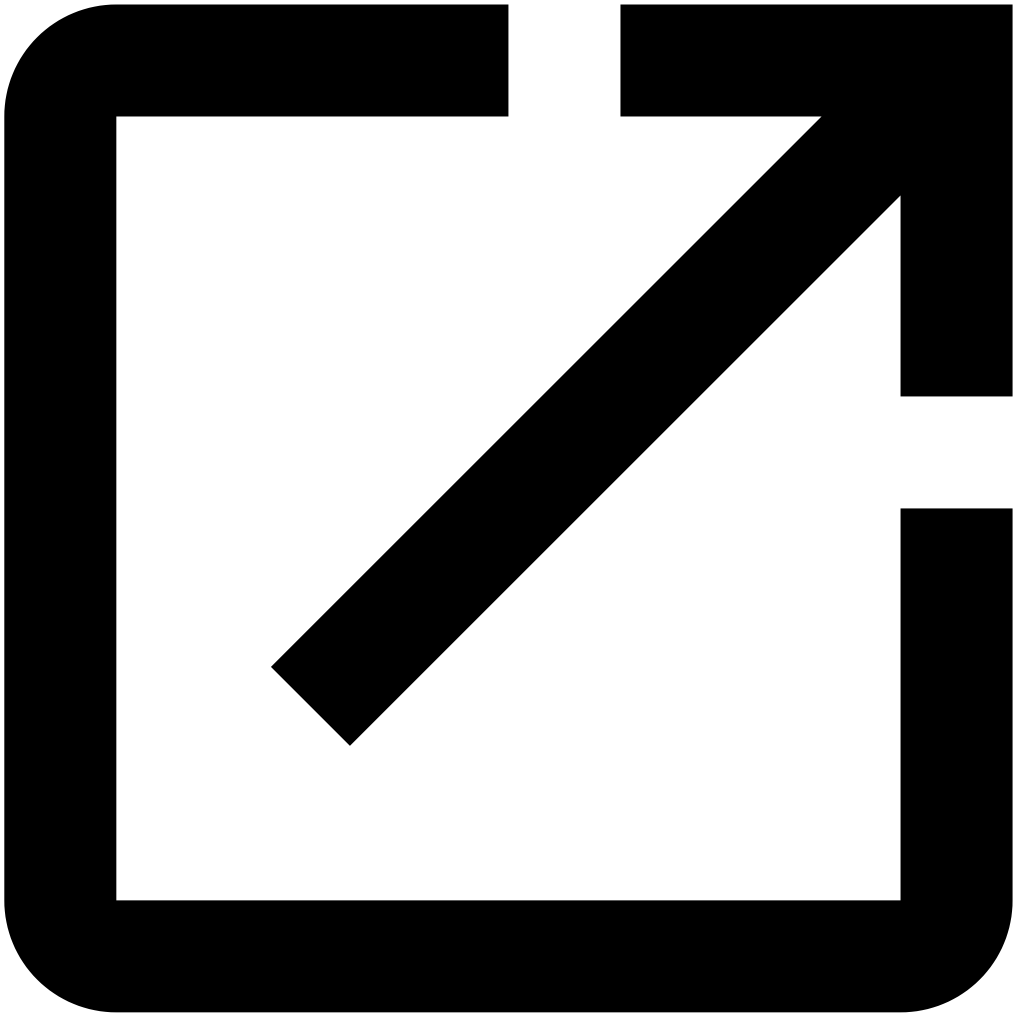
Published: 2020-11-14 · Archived: 2026-04-05 13:20:15 UTC

There were not many known large ransomware attacks this week, but we have seen ransomware operations evolving their tactics to extort their victims further.

The largest attack this week was against Tawainese laptop maker Compal, who was hit by DoppelPaymer. The threat actors are demanding $17 million to receive a decryptor and not to leak stolen files.

Ransomware operations have also begun new tactics this week to pressure their victims into paying a ransom.


DIE LINKE.
0:00



After their attack on Campari, Ragnar Locker hacked a Facebook advertiser's account to run Facebook ads promoting their attack and threatening to release more data. Their strategy is to apply as much pressure as they can on the victim through public awareness in the hopes it will force them to pay the ransom.

Another new tactic announced by DarkSide is their plans to create a fault-tolerant distributed storage service based out of Iran or other "unrecognized republics." Their goal is to use this storage as a platform to leak victim's data for six months, and due to its distributed nature, if one server is shut down by law enforcement, the other servers will still be able to leak the data.

Otherwise, this week has been mostly new variants of existing ransomware families.

Contributors and those who provided new ransomware information and stories this week include: @serghei, @malwrhunterteam, @jorntvdw, @PolarToffee, @VK_Intel, @Ionut_Ilascu, @demonslay335, @LawrenceAbrams, @struppigel, @FourOctets, @malwareforme, @Seifreed, @DanielGallagher, @fwosar, @BleepinComputer, @LukasZobal, @siri_urz, @JAMESWT_MHT, @Unit42_Intel, @briankrebs, @Kangxiaopao, @MsftSecIntel, @campuscodi, @Intel_by_KELA, @briankrebs, and @IntelAdvanced.

November 7th 2020

How Ryuk Ransomware operators made $34 million from one victim

One hacker group that is targeting high-revenue companies with Ryuk ransomware received $34 million from one victim in exchange for the decryption key that unlocked their computers.

When Threat Actors Fly Under the Radar: Vatet, PyXie and Defray777

While researching these malware families, we found that there were several consistencies between Vatet, PyXie and Defray777 that strongly suggest that all three malware families were created, and are currently maintained by, the same financially motivated threat group.

November 8th 2020

November 9th 2020

Fake Microsoft Teams updates lead to Cobalt Strike deployment

Ransomware operators are using malicious fake ads for Microsoft Teams updates to infect systems with backdoors that deployed Cobalt Strike to compromise the rest of the network.

New STOP ransomware variant

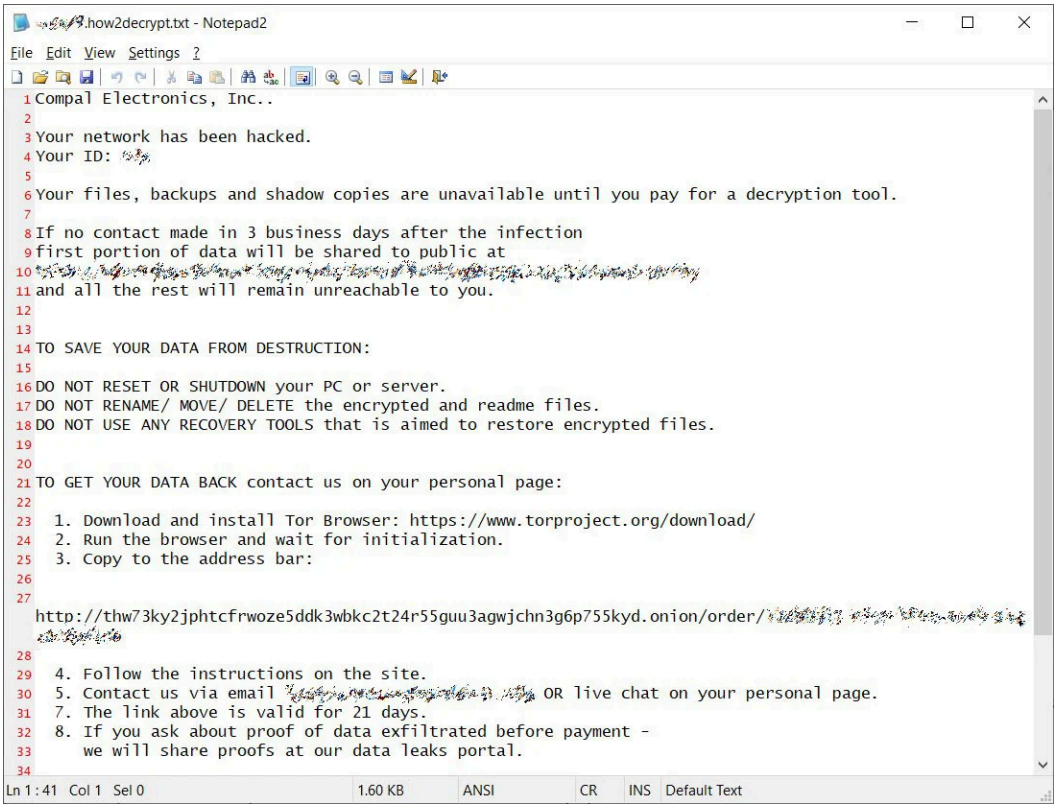
Michael Gillespie found a new STOP ransomware variant that appends the **.agho** extension to encrypted files.

New Dusk 2 ransomware variant

Lukáš Zobal found the new Dusk 2 ransomware variant that appends the **.DUSK** extension to encrypted files and drops a ransom note named **README.txt**.

Laptop maker Compal hit by ransomware, $17 million demanded

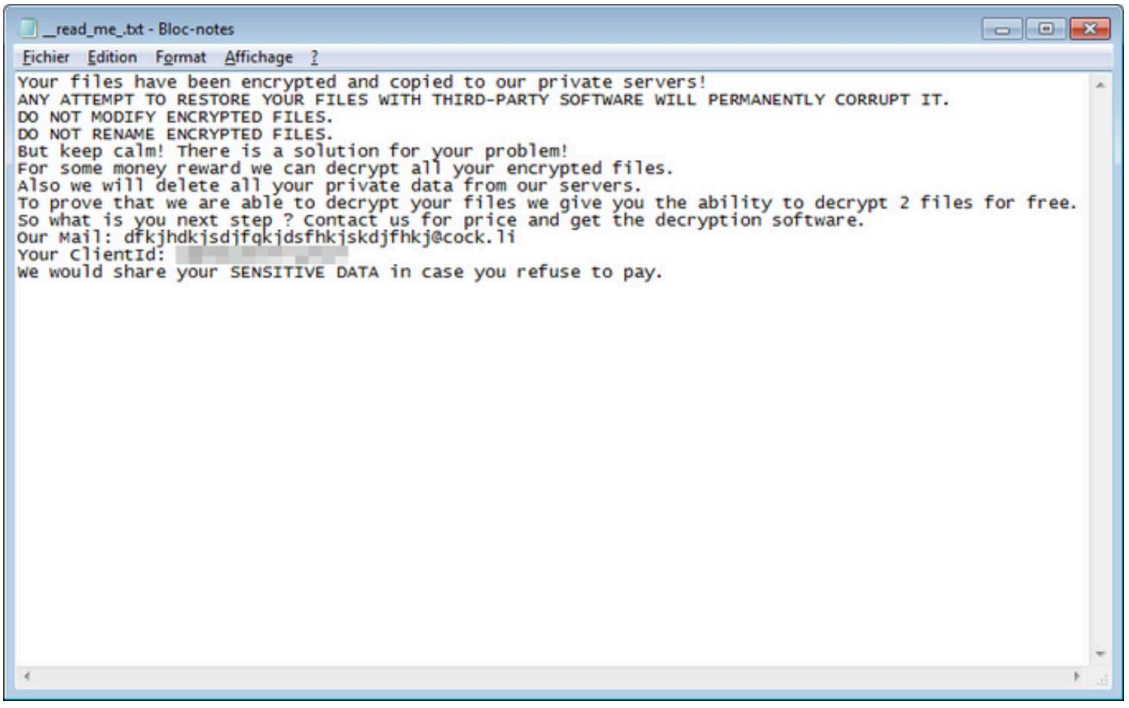
Taiwanese laptop maker Compal Electronics suffered a DoppelPaymer ransomware attack over the weekend, with the attackers demanding an almost $17 million ransom.



November 10th 2020

New HowAreYou Ransomware

S!ri found a new ransomware that appends the **.howareyou** extension to encrypted files.



New AgeLocker ransomware variant

JAMESWT found a new AgeLocker ELF ransomware (targets QNAP devices) that adds the **.kmd** suffix to encrypted files.

November 11th 2020

Recent ransomware wave targeting Israel linked to Iranian threat actors

Two recent ransomware waves that targeted Israeli companies have been traced back to Iranian threat actors.

New Devos Ransomware

xiaopao found a new ransomware that appends the **.devos** extension. This is different than Phobos, which also utilized this extension.

Ransomware gang hacks Facebook account to run extortion ads

A ransomware group has now started to run Facebook advertisements to pressure victims to pay a ransom.

November 12th 2020

Steelcase furniture giant down for 2 weeks after ransomware attack

Office furniture giant Steelcase says that no information was stolen during a Ryuk ransomware attack that forced them to shut down global operations for roughly two weeks.

November 13th 2020

DarkSide ransomware is creating a secure data leak service in Iran

The DarkSide Ransomware operation claims they are creating a distributed storage system in Iran to store and leak data stolen from victims. To show they mean business, the ransomware gang has deposited $320 thousand on a hacker forum.

CRAT wants to plunder your endpoints

Cisco Talos has recently discovered a new version of the CRAT malware family. This version consists of multiple RAT capabilities, additional plugins and a variety of detection-evasion techniques. In the past, CRAT has been attributed to the Lazarus Group, the malicious threat actors behind multiple cyber campaigns, including attacks against the entertainment sector.

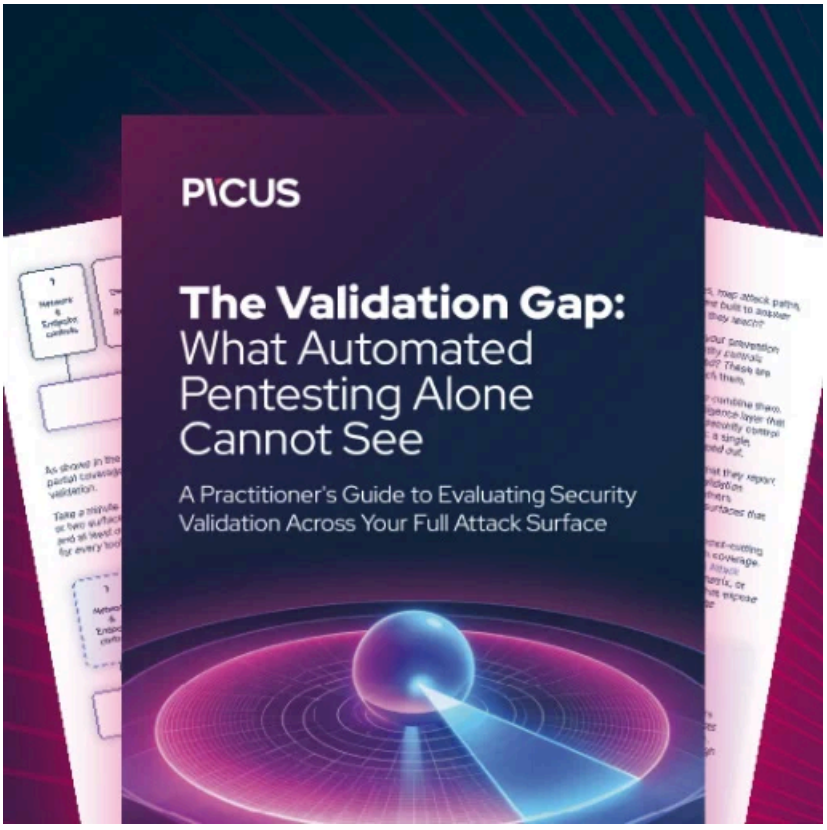
New STOP ransomware variant

Michael Gillespie found a new STOP ransomware variant that appends the .vvoa extension to encrypted files.

LV Ransomware group appears to be using Revil software

Michael Gillespie found a ransomware group known as "LV" utilizing REvil software.

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



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-13th-2020-extortion-gone-wild/