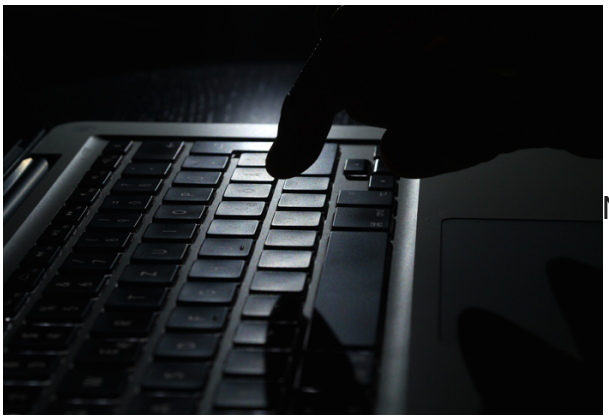
Ransomware Recap: January 14 - 29, 2017

trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-january-14-29-2017



Netflix, with its vast and fast-growing consumer base of over 93 million subscribers in 190 countries, is no stranger to being a subject of cybercriminal activities , with online criminals finding various ways to leverage the streaming service's immense popularity. In the past, we have seen how malefactors used creative methods for stealing credentials that can later on be sold in underground markets, exploit vulnerabilities, and create and distribute malware that enables the theft of user information for profit. Recently, we observed the service being used as a lure, with the promise of a "free Netflix account" as a hook for distributing ransomware.

[Related: Netflix users are becoming favored hacking targets]

In the last week of January, a new ransomware leveraging on the popularity of the video-distribution network was uncovered by researchers highlighting the perils of content piracy. Based on a sample we analyzed, this particular method lures its would-be victim with "free Netflix access" via a supposed login generator for Windows/PC users that, in turn, would lead to the download of a new strain of ransomware (detected by Trend Micro as RANSOM_NETIX.A).

Figure 1: Fake Netflix login generator

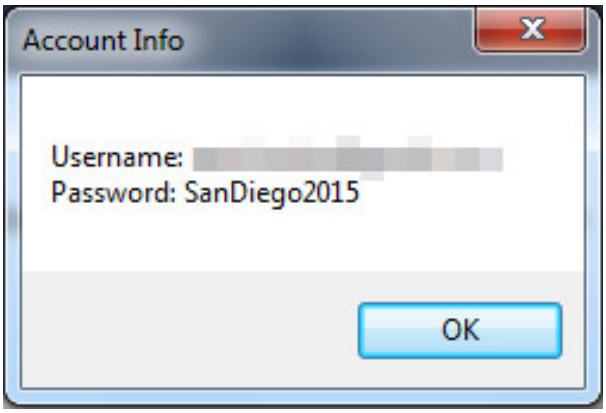


Figure 2: Prompt window of login information from a supposed genuine Netflix account

Typically found on suspicious sites offering cracked applications and unauthorized access to premium membership accounts, this ransomware variant takes the form of an executable named *Netflix Login Generator v1.1.exe* that drops a copy of itself upon execution. The bogus login generator, once clicked by the victim, will prompt another window that displays login information belonging to a genuine Netflix account paired with a fake password. This is done to distract its victim from the ransomware routines running stealthy in the background.

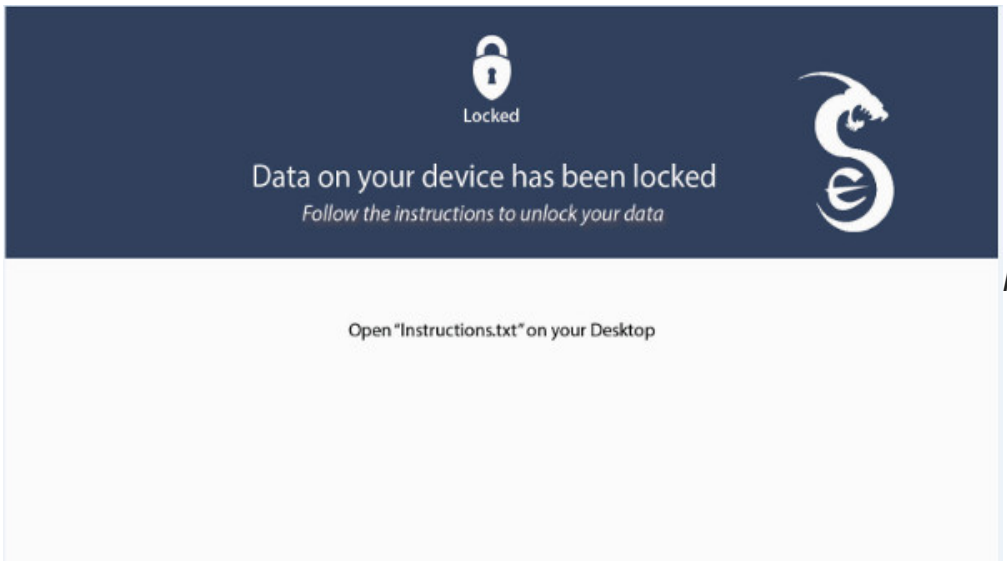


Figure 3: Ransom note displayed as wallpaper

Figure 4: Ransom note containing payment instructions

Using AES-256 encryption, this variant is capable of encrypting 39 file types, appending them with a *.se* extension once done. The ransom will then demand a payment of 0.18 bitcoins, or an amount equivalent to over US$100. Interestingly, the malware will not carry out its routine if the victim's system isn't running on Windows 7 or Windows 10.

Despite the number of social engineering tactics being used to distribute ransomware, these non-technical methods are still proving to be very effective. According to recent reports, a police department in Cockrell Hill, Texas, admitted to being hit by a ransomware infection that cost the department eight years' worth of evidence—an incident that highlighted the importance of implementing a sound backup strategy.

In an initial press release issued by Chief of Police Stephen Barlag, it was noted that the ransomware infiltrated the department's systems early in December of 2016. Following instructions made by the FBI Cybercrimes unit, servers were wiped clean "to ensure that all affected files were deleted". This led to the loss of bodycam, in-car, and department surveillance videos, and some archived photos dating back to 2009.

A more detailed press release dated January 25, 2017 stated that the ransomware in question was named "Osiris", originating from a spam email message that spoofed a legitimate department-issued email address. Security experts believe that the infection was carried out by a ransomware variant with the same name, but the police department could have been hit by a version of Locky (detected by Trend Micro as RANSOM_LOCKY.EXE)—one that appended filenames with an *.osiris* extension. This version emerged shortly after another version of Locky (one that used a .aesir extension) was released, continuing a line of variants that has used extension names alluding to mythological characters, including Odin and Thor.

According to the statement, the ransomware demanded a ransom that amounted to almost $4,000 in bitcoin. In addition to the affected in-house videos and photos, all Microsoft Office suite documents from Word and Excel were affected. While no evidence points to whether any of the affected files were extracted and taken out of the database, the files have all been corrupted and lost. However, the department noted that files stored in DVD and CD format are still accessible.

Days prior to the inauguration of President-elect Donald Trump, another police department got hit by ransomware. According to reports, the attack paralyzed 70% of storage devices that record data for the D.C. police surveillance cameras. Between January 12 and January 15, 123 of 187 network video recorders were affected, forcing the city technicians to wipe its IT systems clean and reboot the devices across the city. Network video recorders are connected to as many as four cameras at each site.

Washington D.C. Chief Technology Officer Archana Vemulapalli said that no ransom was paid. Going into the details of the infection, Vemulapalli noted that the attack impacted only the installed police cameras set up to monitor public areas and did not reach and spread into the D.C. computer networks. Secret Service official Brian Ebert then shared that public safety wasn't compromised.

Not long after this incident, in Europe, a ransomware infection forced officials of four-star Austrian hotel Romantik Seehotel Jaegerwirt to pay the demanded ransom of €1,500 (or US$1,605) in bitcoins. This is the second time the 111-year-old luxury hotel has been hit by a cyber-attack. This is different from previous attacks that focused on extracting payment card details. This time, extortionists prevented hotel admins from programming and issuing room keycards to incoming guests, and left those who left their rooms unable to re-enter.

Managing director Christoph Brandstaetter admitted to caving in to the extortion demand, and shared that plans of reverting to old-fashioned door locks are set to be implemented. Ultimately, the incident serves as a warning to the hotel industry about the importance of security.

Here are other notable ransomware sightings over the past two weeks:

VirLock

When it was first reported, VirLock (detected by Trend Micro as PE_VIRLOCK), was a unique ransomware variant that was not only capable of locking the computer screen but also of infecting files. It targets specific file types to encrypt and infect, from executable, common document, archive, audio/video, image, and certificate files.

It will then stealthily add an .RSRC section to the infected file. This includes the resources used by the executable that are not considered part of the executable, such as icons, images, menus, and strings. This is done to store the resources of the host file, which tricks unsuspecting users into executing the infected files.

Figure 5: Sample ransom note reported in 2015

Before January drew to a close, the variant made a comeback (with samples detected by Trend Micro as PE_VIRLOCK.K and PE_VIRLOCK.K-O), with operations and routines similar to when it was first discovered and reported. This variant encrypts a victim's files and repackages them into an executable file. Because Windows installations do not normally display file extensions, and part of VirLock's routine is to keep the source file's icons, an unsuspecting user could execute the infected files, and worse, unknowingly distribute it to

other users. Interestingly, it was reported that entering a 64-zeroes code to the “Transfer ID” section of the ransomware tricks the malware into believing that the ransom—amounting to $250 in bitcoins—has been paid.

Charger Android Ransomware

Google’s Play Store recently removed a malicious app that reportedly carried a new ransomware variant called Charger (detected by Trend Micro as AndroidOS_ChgLocker.A). According to reports, EnergyRescue, an app disguised as a battery-saving application, gained access and stole a victim’s SMS messages and contact list before locking the user’s device. A ransom note then appeared, threatening to publish collected data online if the ransom is not paid—a routine characteristic of “doxware” as stated below:

You need to pay for us, otherwise we will sell portion of your personal information on black market every 30 minutes. WE GIVE 100% GUARANTEE THAT ALL FILES WILL RESTORE AFTER WE RECEIVE PAYMENT. WE WILL UNLOCK THE MOBILE DEVICE AND DELETE ALL YOUR DATA FROM OUR SERVER! TURNING OFF YOUR PHONE IS MEANINGLESS, ALL YOUR DATA IS ALREADY STORED ON OUR SERVERS! WE STILL CAN SELLING IT FOR SPAM, FAKE, BANK CRIME etc… We collect and download all of your personal data. All information about your social networks, Bank accounts, Credit Cards. We collect all data about your friends and family.

Some of the threats were deemed empty, as there is no evidence that it can exfiltrate information.

Security researchers who looked into Charger note that it possesses sophisticated characteristics that make it different from other Android ransomware variants—particularly the techniques it uses to mask its malicious behavior to bypass detection.

Havoc

Havoc (detected by Trend Micro as RANSOM_HAVOC.A) is a newly-discovered variant that appends affected files with the *.HavocCrypt* extension name. This variant performs routines typical of a ransomware type that uses symmetric and asymmetric cryptography to encrypt its targeted files.

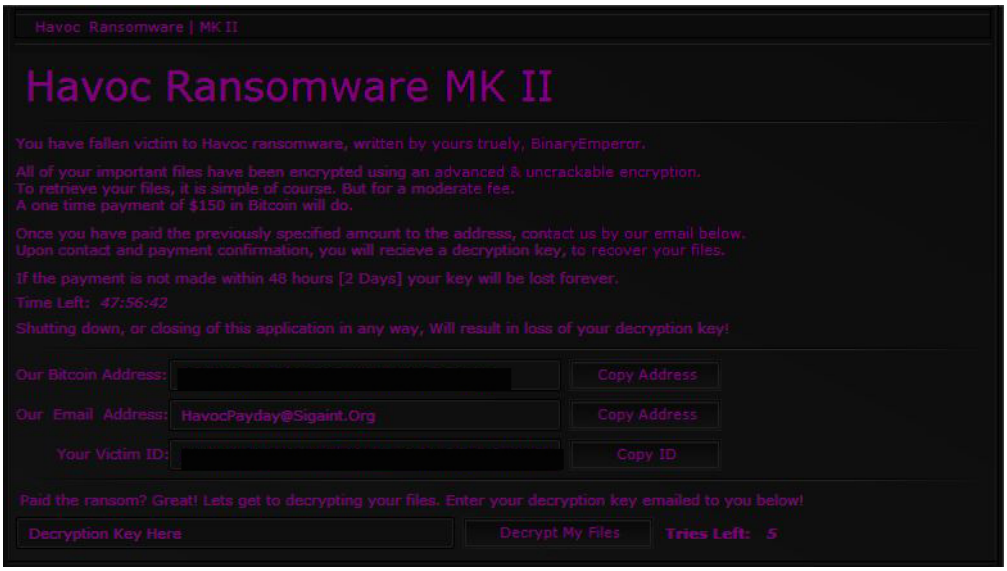


Figure 6: Havoc ransom note

A ransom of $150 in bitcoins comes with a 48-hour deadline. Failure to do so would result in the permanent deletion of the decryption key provided by the online criminals. Apart from a countdown timer, the ransom note also indicates that any form of attempt to close or shut down the ransomware application will also lead to the deletion of the decryption key.

VxLock

Also discovered in the last two weeks is a new ransomware (detected by Trend Micro as RANSOM_VXLOCK.A) named after the extension name it adds to the files it encrypts. With attributes common to ransomware variants seen in the past, this variant targets files and appends the extension name *.vxlock* to its encrypted file, renaming a locked Word document with the file name file.doc into *file.doc.vxlock*.

While researchers observe that this variant is set to undergo further development, it is notable that at this stage, Vxlock has AntiVM, Anti-debug and Anti-Sandbox features.

```
internal class vxAnti
{
    private bool antidebug;

    private bool antisandbox = true;

    [DllImport("kernel32.dll")]
    private static extern bool IsDebuggerPresent();

    [DllImport("kernel32.dll")]
    private static extern bool CheckRemoteDebuggerPresent(IntPtr hProcess, ref bool isDebuggerPresent);

    [DllImport("kernel32.dll")]
    public static extern IntPtr GetModuleHandle(string lpModuleName);

    public vxAnti()
    {
        if (this.antidebug)
        {
            this.AntiDebug();
        }
        if (this.antisandbox)
        {
            this.DetectSandboxie();
        }
    }

    private void DetectSandboxie()
    {
        if (vxAnti.GetModuleHandle("SbieDll.dll").ToInt32() != 0)
        {
            Environment.Exit(102);
        }
    }

    protected void AntiDebug()
    {
        if (vxAnti.IsDebuggerPresent())
```

Figure 7: Vxlock Anti-AV checking

Crypto1CoinBlocker

This particular variant (detected by Trend Micro as RANSOM_XORIST) surfaced as an updated version of an earlier released ransomware, Xorist. Using RSA-2048 cryptography, it targets affected system's files and appends random alpha-numeric numbers serving as the victim's dedicated Bitcoin wallet address to the file name of the encrypted file. Following encryption, it displays a fake error message, a pop-window, and a text file placed on the desktop, all signaling compromised data.

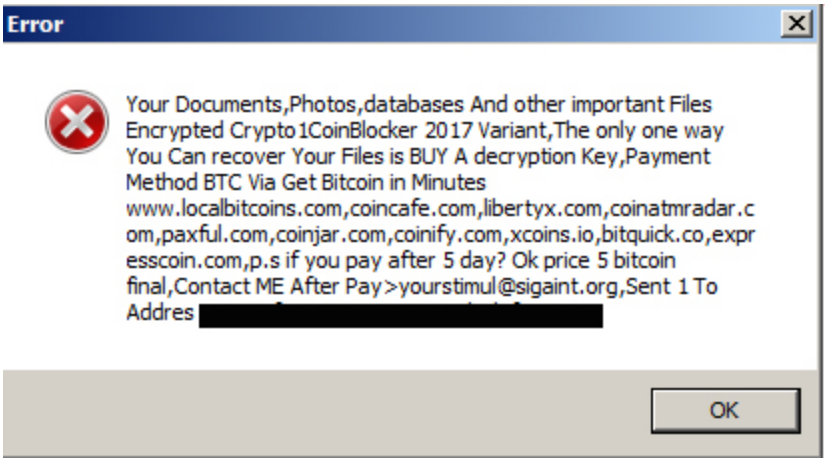


Figure 8: Fake error message

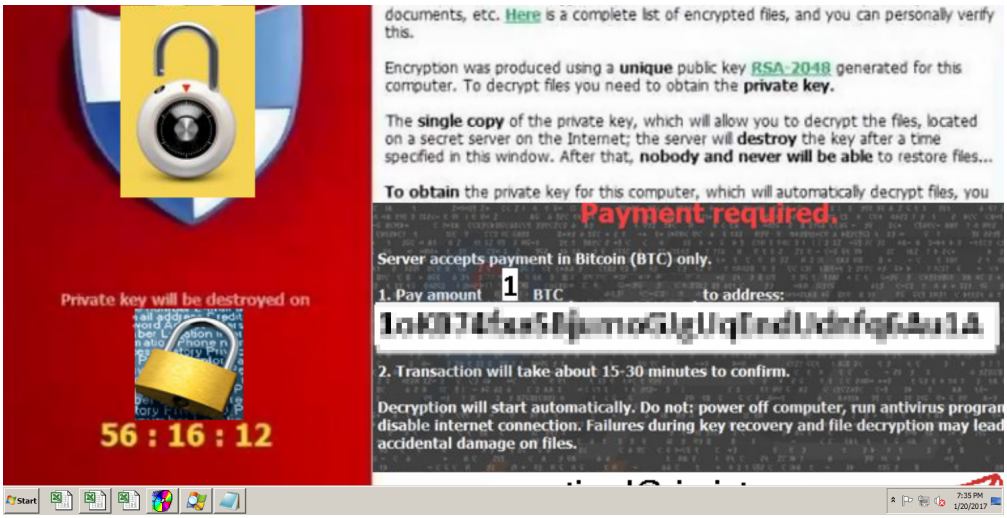


Figure 9: Ransom note replacing the system's wallpaper

The fake message, appearing after the locking of files was carried out alerts the victim to pay a hefty sum of 5 bitcoins or an amount reaching almost US $ 5,000. Clicking “OK” to the message would prompt the desktop to display a new wallpaper that interestingly asks for a smaller ransom of 1 bitcoin—almost $1,000—to be settled within a given time frame.

A multi-layered approach is key to defending all possible gateways from malware. IT administrators in organizations should empower the workforce with necessary education to keep employees well informed of attack tactics. On the other hand, a solid back-up strategy of important files significantly mitigates damages brought by a ransomware infection.

Ransomware solutions:

Trend Micro offers different solutions to protect enterprises, small businesses, and home users to help minimize the risk of getting infected by ransomware:

Enterprises can benefit from a multi-layered, step-by-step approach in order to best mitigate the risks brought by these threats. Email and web gateway solutions such as Trend Micro™ Deep Discovery™ Email Inspector and InterScan™ Web Security prevents ransomware from ever reaching end users. At the endpoint level, Trend Micro Smart Protection Suites deliver several capabilities like high-fidelity machine learning, behavior monitoring and application control, and vulnerability shielding that minimizes the impact of this threat. Trend Micro Deep Discovery Inspector detects and blocks ransomware on networks, while Trend Micro Deep Security™ stops ransomware from reaching enterprise servers–whether physical, virtual or in the cloud.

For small businesses, Trend Micro Worry-Free Services Advanced offers cloud-based email gateway security through Hosted Email Security. Its endpoint protection also delivers several capabilities such as behavior monitoring and real-time web reputation in order detect and block ransomware.

For home users, Trend Micro Security 10 provides strong protection against ransomware by blocking malicious websites, emails, and files associated with this threat.

Users can likewise take advantage of our free tools such as the Trend Micro Lock Screen Ransomware Tool, which is designed to detect and remove screen-locker ransomware; as well as Trend Micro Crypto-Ransomware File Decryptor Tool, which can decrypt certain variants of crypto-ransomware without paying the ransom or the use of the decryption key.

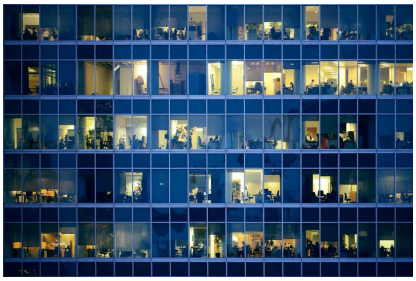
HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

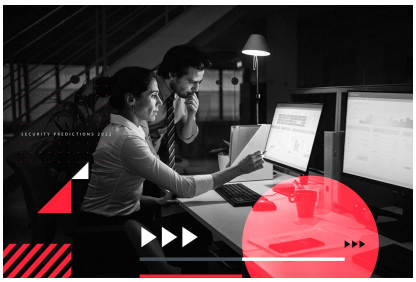
Posted in Cybercrime & Digital Threats, Ransomware

2021 Midyear Cybersecurity Report



In the first half of this year, cybersecurity strongholds were surrounded by cybercriminals waiting to pounce at the sight of even the slightest crack in defenses to ravage valuable assets.
View the report

Trend Micro Security Predictions for 2022: Toward a New Momentum



In 2022, decision-makers will have to contend with threats old and new bearing down on the increasingly interconnected and perimeterless environments that define the postpandemic workplace.
View the 2022 Trend Micro Security Predictions