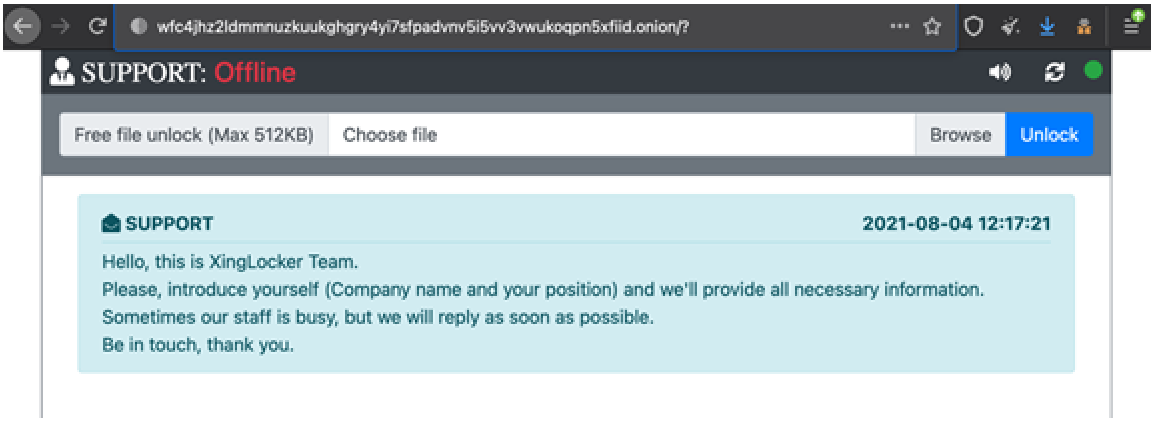
Ransomware Operators Found Using New "Franchise" Business Model

trendmicro.com/en_us/research/21/j/ransomware-operators-found-using-new-franchise-business-model.html

October 15, 2021



wfc4jhz2ldmmnuzkuukghgry4yi7sfpadvnv5i5vv3vwukoqpn5xfiid.onion/?
SUPPORT: Offline
Free file unlock (Max 512KB)
Choose file
Browse
Unlock

SUPPORT 2021-08-04 12:17:21

Hello, this is XingLocker Team.
Please, introduce yourself (Company name and your position) and we'll provide all necessary information.
Sometimes our staff is busy, but we will reply as soon as possible.
Be in touch, thank you.

Shared infrastructure

To date, we have found fifteen onion addresses used by at least four different servers, and three others still unknown.

Onion Address	**Server**
w6ilafwwrgtrmilorzqex6pgpvfsa667fydca2wpoluj6sajka225byd[.]onion	A
accdknc4nmu4t5hclb6q6kjm2u7u5xdzjnewut2up2rlcfqe5lootlqd[.]onion	A
c6zkofycoumltpmm6zpyfadkuddpmlqk6vyd3orrfjgtq3vrgyifl6yd[.]onion	A
3klsbd4dwj3yqgo4xpogfgwqkljbnbdxjryeqks2cjion5jj33wvkqyd.onion	B
yk7erwdvj4vxcgiq3gmcufkben4bk4ixddl5j2xvu7gurtdq754jmiad.onion	B
z4cn6lpet4y4r6mdlbpklpcrjdruwb6kiuvxn6gsiuoub23z6prlx6ad.onion	B
ibih5znjxf2cqgo737xmooyvmxhac45wd4rivh6n5hd7fysn42g3fayd.onion	B
ikrah6fb4e6r2raxkyvyoxp22jam5z6ak5ajfnzxutmassoagvr2bhad.onion	B
hceesrsg6f5p4gcph4j6jv6vl4mkmaik735oz4r45lgjfyedsxfoprad.onion	B
qfgh2lpslhjb33z3wsenmqrxcdragelinvcpowlgkbjca6yig5zloeyd.onion	B

x4mjvffmytkw3hyu.onion	C
tpze4yo74m6qflef.onion	D
evl425tkt4hkwryyplvqu6bn6slfow3fa4xwgvwe5t4zf6gizs3ewuyd.onion	Unknown 1
xingnewj6m4qytljhfwemngm7r7rogrindbq7wrfeepejgxc3bwci7qd.onion	Unknown 2
zckdr5wmbzxphoem77diqb2ome2a54o23jl2msz3kmotjlpdnjhmn6yd.onion	Unknown 3

Table 1. The onion addresses used by the different servers

And here is how they relate to the group:

Server	XingLocker	AstroLocker Team
A	x	
B	x	x
C	x	x
D	x	
Unknown 1	x	
Unknown 2	x	
Unknown 3	x	

Table 2. The different servers in relation to XingLocker and AstroLocker Team

While this is not a sophisticated innovation, it is important to highlight that ransomware groups are looking for new ways to run their affiliate programs and RaaS businesses. This form of shared infrastructure and code can make things harder from an investigative point of view. It is not uncommon to find XingLocker samples detected as Mount Locker, or identify two different onion addresses pointing to the same onion service but used by different groups. Investigators should be aware of these factors when researching ransomware.

Why is this important? Most RaaS models operate by affiliates working with the ransomware group to install a specifically named ransomware on as many machines as possible, then splitting the profits. This is advantageous for the attackers because when victims look up the ransomware and see many reports about it, they are more likely to pay. As a disadvantage, affiliates are largely anonymous and can’t use these attacks as the basis of THEIR own criminal business. They are just like managers in a burger chain.

It seems likely we have now observed a new "franchise" RaaS model involving XingLocker, AstroLocker and Mount Locker. In this model there seems to be a main RaaS (in this case Mount Locker), and then affiliates license the ransomware and release it under their own name and brand.

In this scenario, the affiliates are like managers of their own local burger joint, getting products from a generic food supplier. The products are provided by the parent company, but the individual operators conduct business under their own branding, with unique names and images. This method gives more flexibility and recognition for the affiliates, especially mid-tier aspiring criminal gang leaders. One disadvantage is that it means less brand recognition for specific ransomware, so victims may be less inclined to pay. Of course, from an investigation point of view, this method adds confusion in terms of naming and makes tracking harder.

How to Defend Against Ransomware

Ransomware is a continuously evolving threat, and organizations should be vigilant in maintaining the best and most effective security policies and practices. Protection frameworks set by the Center of Internet Security and the National Institute of Standards and Technology can help organizations prevent and mitigate the impact of ransomware attacks:

- Audit and inventory: Take an inventory of all organizational assets and data, and identify authorized and unauthorized devices, software, and personnel accessing particular systems. Audit and monitor all logs of events and incidents to identify unusual patterns and behaviors.
- Configure and monitor: Deliberately manage hardware and software configurations, and only grant administrative privileges and access to specific personnel when absolutely necessary. Monitor the use of network ports, protocols, and services. Implement security configurations on network infrastructure devices such as firewalls and routers, and have a software allow list to prevent malicious applications from being executed.
- Patch and update: Perform periodic vulnerability assessments, and conduct regular patching or virtual patching for operating systems and applications. Ensure that all installed software and applications are updated to their latest versions.
- Protect and recover: Enforce data protection, backup, and recovery measures. Implement multifactor authentication in all devices and platforms used whenever available.

- Secure and defend: Perform sandbox analysis to examine and block malicious emails. Employ the latest version of security solutions to all layers of the system, including email, endpoint, web, and network. Spot early signs of an attack such as the presence of suspicious tools in the system, and enable advanced detection technologies such as those powered with AI and machine learning.
- Train and test: Perform security skills assessment and training for all personnel regularly, and conduct red-team exercises and penetration tests.

Trend Micro Solutions

Organizations can benefit from security solutions that encompass a system’s multiple layers (endpoint, email, web, and network) not only for detecting malicious components but also for close monitoring of suspicious behaviors in the network.

Trend Micro™ Vision One™ provides multilayered protection and behavior detection, spotting questionable behaviors that might otherwise seem benign when viewed from only a single layer. For an even closer inspection of endpoints, Trend Micro Apex One™ offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware. This allows detecting and blocking ransomware early on before it can do any real damage to the system.

With techniques such as virtual patching and machine learning, Trend Micro™ Cloud One™ Workload Security protects systems against both known and unknown threats that exploit vulnerabilities. It also takes advantage of the latest in global threat intelligence to provide up-to-date, real-time protection.

Ransomware often gets into the system through phishing emails. Trend Micro™ Deep Discovery™ Email Inspector employs custom sandboxing and advanced analysis techniques to effectively block ransomware before it gets into the system.

For the Indicators of Compromise, please see this document.

Ransomware

We found a relatively new and interesting ransomware operation that takes inspiration from franchise business models. It seems that the operators are rebranding a "supplier" ransomware before deployment instead of simply distributing it under the original name.

By: Fernando Merces October 15, 2021 Read time: (words)

Content added to Folio