A (R)Evil Cybercrime Gang Disrupting Organizations for Trade Secrets and Cash

securityintelligence.com/posts/sodinokibi-revil-ransomware-disrupt-trade-secrets/

Home&nbsp/ Incident Response

The Sodinokibi Chronicles: A (R)Evil Cybercrime Gang Disrupts Organizations for Trade Secrets and Cash

Incident Response April 28, 2021
By Limor Kessem 9 min read
It likes big game hunting, it enjoys deploying Cobalt Strike and it dabbles in critical vulnerability abuse. It's known as Sodinokibi/REvil, a ransomware strain that emerged in 2019 as the heir to the GandCrab ransomware, a malware family that supposedly retired from the cyber crime arena in mid-2019 after reportedly amassing illicit profits of over $2 billion.

In the two years of its existence, Sodinokibi has gained considerable momentum, having been implicated in high-profile cyberattacks, locking up and even auctioning off data that belonged to companies like Travelex, Gunnebo, Brown-Forman, Asian retail giant The Dairy Farm Group and, most recently, an Apple supplier. The demand in each case is often exorbitant, asking victims for multi-million-dollar ransoms for their data:

- Leading cosmetics group Pierre Fabre: $25,000,000
- The Dairy Farm Group: $30,000,000
- New York-based law firm Grubman Shire Meiselas & Sacks: $42,000,000
- Apple MacBook supplier: $50,000,000

Is Sodinokibi all about the money? It's hard to say. In some cases, Sodinokibi actors manage to target defense contractors and organizations in countries that rival their assumed originating state, Russia.

Robbing terabytes of data, with no way for victims to know what they actually do with it after they receive payment, it's very plausible that money is just one objective, followed by espionage, both business and nation-state driven. Not unlike other major cybercrime gangs, the group's access and control over major organizations' assets can lend it the power to collaborate on a variety of nefarious schemes, including adversarial nation-state activity.

'Cryptoviral Extortion' Is the Name of the Game

Threat actors that use ransomware are taking advantage of the inherent power of public key infrastructure cryptology to encrypt information in a way that's hard or impossible to break. The term "cryptoviral extortion" was coined in 1996 in an Institute of Electrical and Electronics Engineers (IEEE) paper. The IEEE also predicted that cryptoviral extortion would one day demand 'e-money,' long before Bitcoin even existed.

For the cryptographic basis of the attack, Sodinokibi uses a combination of elliptic curve Diffie-Hellman (ECDH), Salsa20, SHA-3 and Advanced Encryption Standard (AES) to encrypt and decrypt both malicious configuration data and user data (i.e., user files). It generates its private-public key pair using Curve25519, one of the fastest elliptic-curve cryptography (ECC) curves designed for use with the ECDH key agreement scheme.

Sodinokibi operators may steal data in advance and then resort to extortion tactics that exceed the ability of the malware itself. Those who refuse to pay up, relying on their ability to recover data, will then receive threats to have that data exposed on an auction site the group calls The Happy Blog. That's also where it names and shames its victims, offering up information that could be of use to other criminals or even competitors.

Additionally, in an interview given by an alleged REvil operator, known as Unknown, the person said he/she was considering launching distributed denial-of-service (DDoS) attacks on victim organizations as yet another way to increase the pressure on victims to pay the ransom.

In terms of prevalence in the wild, Sodinokibi made up 22% of all X-Force incident response engagements in 2020, suggesting that those operating this malware are more skilled at gaining access to victims' networks when compared to other ransomware strains. X-Force estimates that nearly 80% of the gang's victims are a combination of organizations from the US (58%), UK (8%), Australia (5%) and Canada (3%).

The faces of Sodinokibi are many, as it is the sort of malware that's distributed by various affiliates. In 2020, this ransomware's originators showed off their success by depositing $1 million in Bitcoin into a Russian-speakers' cyber crime forum as part of a recruitment drive for more affiliates to join its ranks.

Sodinokibi: A Head-to-Head Battle With Manual Targeted Attacks

Once Sodinokibi focuses on a potential victim, the attack goes into a more sophisticated operation by human actors who pave their way through the compromised networks to find data, exfiltrate it and sow the seeds of the ransomware phase across as many devices as possible. This is a major issue since it's harder to detect a careful human who can change tactics according to what's happening on the defenders' side.

That has not restricted the number of attacks by the group of Sodinokibi operators. The number of publicized attacks is likely the tip of an iceberg. According to X-Force data from 2020, we estimate the total victim count to be around 250 organizations. Our most conservative estimate places the total Sodinokibi ransom revenue at $123 million in 2020. This estimate is the result of several factors, notably the big game hunting attacks. Of the estimated 19 victim organizations with total annual revenue of $1 billion or more, at least 15 have probably paid a multi-million-dollar ransom.

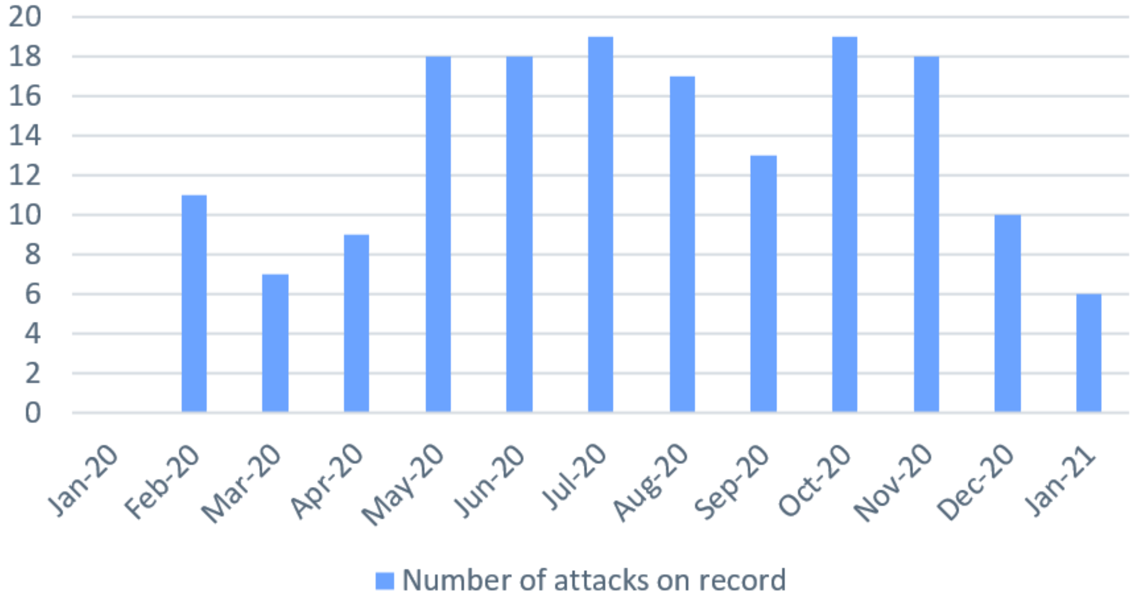


Figure 1: Attacks per month (Source: IBM X-Force)

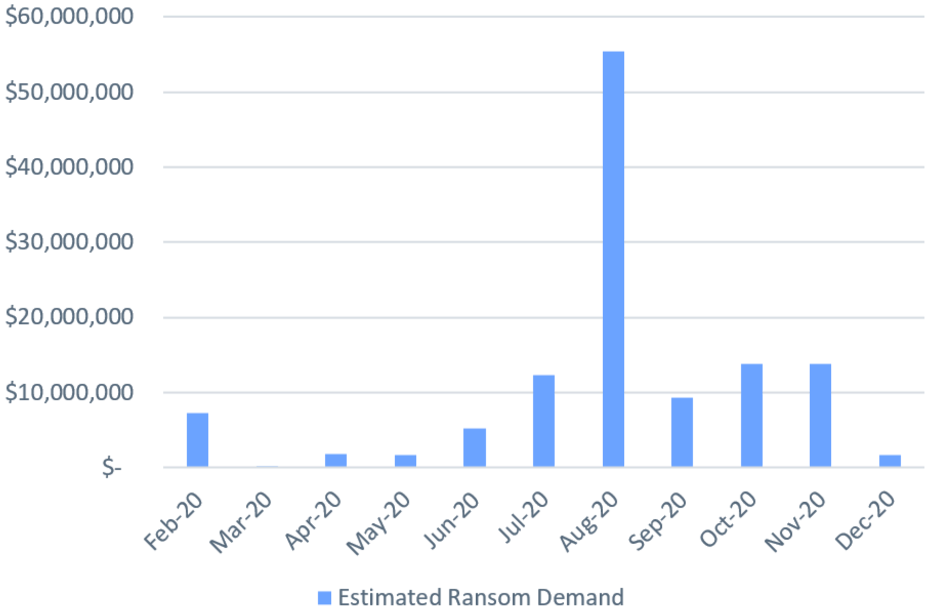


Figure 2: Ransom demands per month (Source: IBM X-Force)

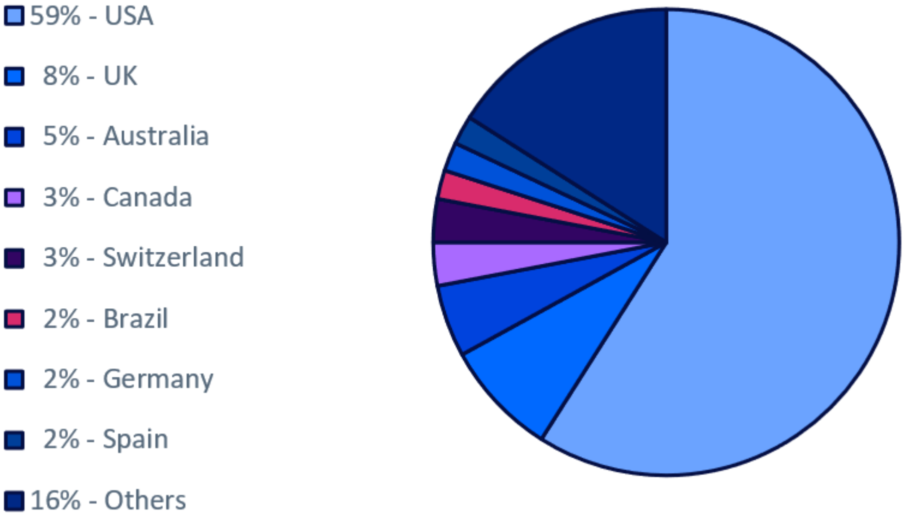


Figure 3: Victimized organizations by geo-location (Source: IBM X-Force)

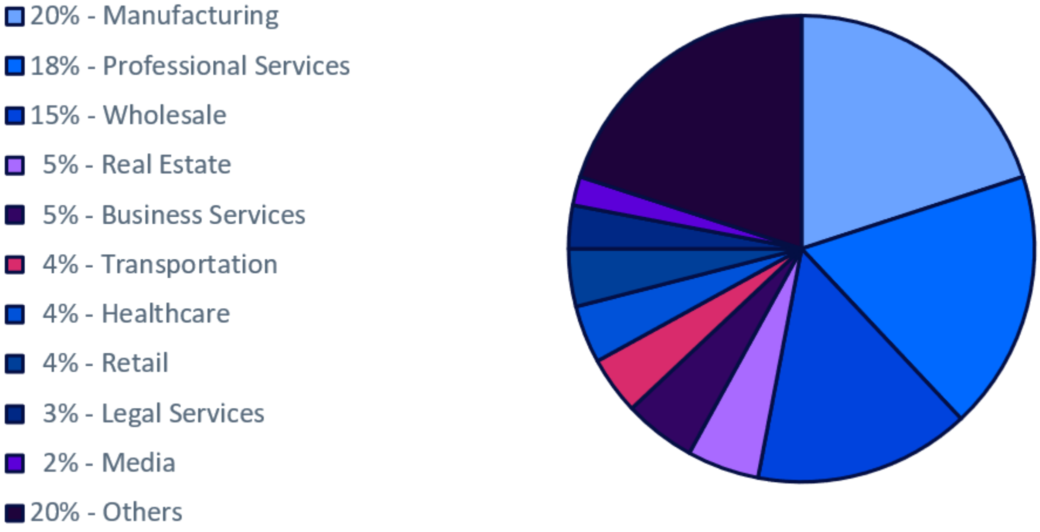


Figure 4: Victimized organizations by industry (Source: IBM X-Force)

The Price of Trust

According to IBM Security surveys and data collected on ransomware attacks, at least half of organizations targeted with ransomware pay the ransom. That model might have worked in some cases, in the past, when the only threat was locked files. But, a new question arises: Are cyber criminals breaking their own business model by challenging organizations to trust them with their stolen data?

With blended attacks that both steal and encrypt data, cyber criminals can add pressure to their scheme and force organizations to pay or have their data exposed or auctioned off. But, in reality, the minute a copy of confidential data is outside the organization, there is no telling what's actually being done with it. Is it truly being deleted? This is not a predicament any organization would choose to be in. In some Sodinokibi cases, the attackers who were supposed to delete the stolen data after they got paid ended up coming back for seconds, demanding more money be paid because they kept the data.

This raises the espionage question once again. After the ransom is paid for the decryption and supposed deletion of the stolen data, who's to guarantee that the same data is not then offered anonymously to a competitor? Who's to say it won't be offered to a rivaling nation-state for a hefty fee, all under the cloak of cryptocurrency payments and money-laundering capacity that cyber crime gangs build by fostering relationships with other organized crime groups?

There are no guarantees. A decryption key is one thing, buying trust is another. That's why this may seem like bad news at first sight, but it could be a factor that will make organizations less inclined to pay ransoms.

With gangs like Sodinokibi thinking of expansion and attack diversity, security executives are better off looking at security reinforcements and preventive measures (i.e., encrypting data so it is useless if stolen, safely storing backups, threat intelligence-driven patch vulnerability strategy, data loss prevention, continuous zero-trust improvements, etc.) rather than dumping millions of dollars into a losing game — an attacker's bottomless pocket.

It's Sodinokibi — What's Next?

When a ransomware attack is discovered, every second counts. As time passes, more data and files are being encrypted, driving up the cost and damage of that attack. Immediate — yet methodical and informed — action must be taken.

A first move should be involving IT security teams and allowing them to launch the incident response process that they have prepared to combat ransomware. If you have a retainer contract with a third-party provider, it is advisable to engage them now and get responders on site. In the meantime, all defensive actions should count on the assumption that the attacker is still in the environment and monitoring all communications.

If your team figures out which malware has encrypted data, typically by the encrypted file extensions, run an initial root cause analysis (RCA) to determine how the malware got in. While a formal RCA can wait until the post-incident activity phase, an abridged RCA will aid the organization in entering the containment phase. Without a basic RCA, the infection cycle is more likely to repeat itself. It is also important to perform the RCA before the recovery phase, since an organization could expend a large amount of time and effort recovering files only to see them re-encrypted shortly thereafter.

The pressure is on, the attackers make every possible threat at this point, and time is running out quickly. If data has been stolen (e.g., customer data, financial data, cyber insurance information, intellectual property, etc.) and the organization understands what's at stake, the company's counsel, data privacy officer (DPO) or privacy officer should be involved to plan the response that concerns customers and data subjects. Other parties to consider contacting are federal law enforcement and regulators, depending on the local requirements for the industry and geographies in which your company operates.

Fast forward to the recovery stage, as this is the point at which companies will typically consider cutting their losses and may plan on paying the ransom or negotiating it down. It's important to consider the newer pressure tactics Sodinokibi operators use on top of encryption, data exfiltration and DDoS, before paying. Moreover:

- Paying a ransom does not guarantee recovery; some data may have been corrupted.
- Paying a ransom does not equal instant recovery; it may take weeks or months to decrypt data.
- Paying a ransom can be a federal offense if paid to attackers in certain countries.
- Paying organized cyber crime operations like Sodinokibi funds and strengthens their business model.

Sodinokibi Expanding in 2021

Sodinokibi actors have been trying to recruit additional affiliates. One way to lure new members to collaborate with them is by flaunting their wealth, by depositing $1 million in a Russian-speaking underground forum, to assure members they can be trusted and those who join will get paid.

The types of skills the group is after, and those which defenders will be seeing more of in 2021, appeared in a post in a dark web forum.

"Groups that have already got expertise and expertise in penetration testing, working with MSF (aka MetaSploit Framework)/CS (aka Cobalt Strike)/Koadic (a Windows post-exploitation framework and penetration testing tool), NAS/Tape (enterprise data archiving and storage), Hyper-V, and analogues of the listed software programs…"

On top of these popular ransomware tactics, techniques and procedures (TTPs), check out the annex at the end of this blog post for additional cues.

At this time, no end is in sight for Sodinokibi, but that does not mean it will not suddenly shut down operations and disappear. In some cases, cyber criminals bow out of the arena when they have amassed considerable wealth and are worried about potential law enforcement crackdowns. We have seen such occurrences with GandCrab in 2019, Maze ransomware in late 2020 and FonixCrypter in January 2021.

Until that happens with Sodinokibi — and with no reason to doubt that new actors will rise next — defenders should continue to focus on security and employee awareness to limit the potential for these types of attacks.

Facing a Sodinokibi Attack?

If your team requires assistance, please contact the X-Force hotlines:

North America: 24×7 Hotline: 1-888-241-9812

Global Hotline: +00 1 (312) 212-8034

IBM X-Force Threat Intelligence

IBM X-Force IRIS Threat Intelligence Solutions offers global intelligence experts, analysis and platform integration of threat intelligence into security workflow applications.

IBM X-Force Incident Response Services

Incident response services — retainer subscription and proactive services to reduce incident response time, minimize breach impact and help you recover faster.

ANNEX

General Ransomware Characteristics to Look Out For

Ransomware attackers, including Sodinokibi actors, tend to be sophisticated, stealthy and prevalent. Most times, they seek to gain access to a victim organization's network by either exploiting a vulnerability or acquiring and abusing valid account credentials.

Obtaining that initial set of account credentials typically comes through phishing attacks or purchases in dark web cyber crime forums. Ultimately, once an attacker gains an initial foothold, they seek to move laterally and acquire as many privileged account credentials as possible. The use of some malware or penetration testing tools is a common practice.

Common Infection Vectors (e.g., vulns. exploits)

- Phishing/malware
- Vulnerability exploitation
- Open/poorly secured RDP

Commonly Exploited Vulnerabilities to Prioritize

- RDPs
  - BlueGate CVE-2020-0609, CVE-2020-0610
  - CVE-2020-16896
  - CVE-2019-1225
  - CVE-2019-1224
  - CVE-2019-1108
- CVE-2019-19781 Citrix
- CVE-2019-2725 Oracle WebLogic
- CVE-2020-2021 Palo Alto Firewall
- CVE-2020-5902 F5 BIG-IP
- CVE-2018-8453 (EoP) Windows (RCE) win32k.sys
- CVE-2020-1472 Windows Netlogon ZeroLogon (post-initial foothold/compromise)
- VPNs
  - CVE-2019-11510 Pulse Secure Connect
  - CVE-2019-11539 Pulse Secure Connect
  - CVE-2018-13379 FortiOS SSL VPN
  - CVE-2019-18935 Telerik UI (JuicyPotato exploit)

Common Capabilities

- Antivirus and sandbox evasion/anti-debug, anti-analysis tricks
- Binary file is encrypted
- CRC32 checks
- Process injection tactics
- API hashing/dynamic API resolution
- Mount and encrypt virtual disks (e.g. virtual machine files like VHD, VHDX)
- UAC bypass
- Wake-on-Lan (WoL)
- Process doppelgänging
- Deploy and execute ransomware inside its own virtual machine container
- Disable Windows driver signature enforcement
- Kill specific running processes and services
- Delete data, e.g., various logs (attack evidence), volume shadow copies, backups, etc.
- Disable/delete various system security settings (e.g., Windows firewall, Windows Defender definitions, etc.)
- Evade detection, e.g., msbuild.exe, Heaven’s Gate technique, use memory mapped I/O to encrypt each file, etc.
- Rapid, multithread encryption

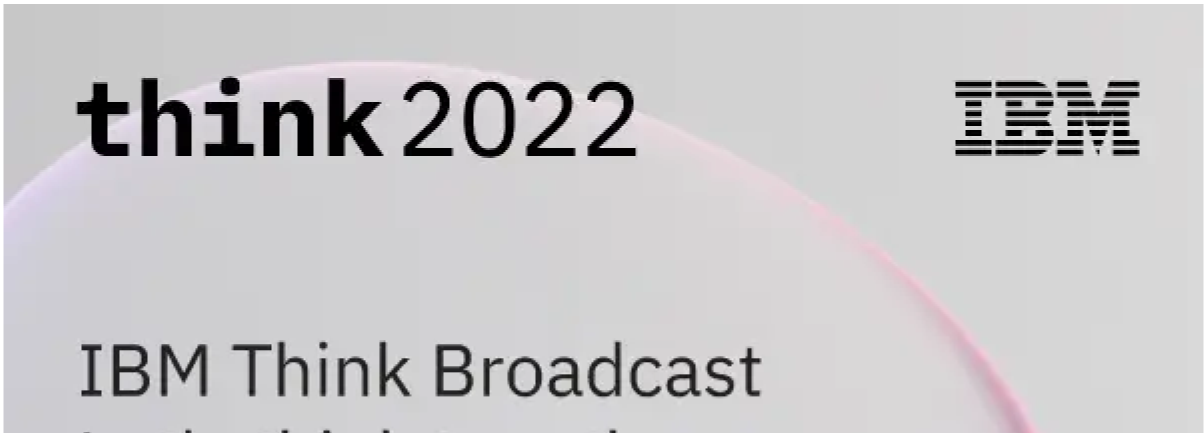
Common TTPs to Look Out For

- Harvesting privileged account credentials, admins of varying sorts.
- Use of legitimate, remote access software like AnyDesk, NetSupport Manager, etc.

- Use of PuTTY Link (aka Plink) to tunnel RDP sessions and establish connections to other devices on the network with randomized source and destination ports.
- Creation of one or more user accounts and/or groups, group policies (GPOs).
- Attempts to encrypt network shares; creates new tasks, registry keys
- Attacker will target systems with V-sphere/ESXi/Nagios, NAS (data exfil), network shares (data exfil), Exchange server (monitor and steal internal communications) and consolidated backups (which can frustrate recovery efforts) especially during the internal reconnaissance phase.
- Internal network scans looking for IP ranges with the following services/ports:
    - 10.0.0.0-10.0.255.255
    - HTTP and proxy (ports 80, 443, 3128, 8080)
    - FTP and SFTP (port 21, 115)
    - Database servers (ports 1433, 3050, 3306)
    - Remote management (ports 22, 23, 3389, and 4899)
- Log deletion using publicly available code.
- Lateral movement — many times, a primary subgoal is to move to a domain controller (DC).
    - PSremoting session started; PowerShell downloads scripts and files; privileged account used (i.e., Domain Admin); ADrecon executed (reconnaissance); Scheduled Task executes script from SystemApps; lateral movement via Cobalt SMB beacon.
    - Once on a DC, attackers attempt to disable Windows security settings like MS firewall settings for all domain-joined computers via new GPO.
    - Deployment and detonation of ransomware on all domain-joined computers via GPO.
- Watch for any network activity to/from cloud storage platforms as a way by which data is being exfiltrated.

Limor Kessem
Executive Security Advisor, IBM

Limor Kessem is an Executive Security Advisor at IBM Security. She is a widely sought-after security expert, speaker and author and a strong advocate for wom...



Let's think together.

Watch on demand →