

THE MONITOR

VOLUME 3

**Sodinokibi
Ransomware: A
New Strain Takes
the Stage**

PAGE 2

**Ransomware on
the Rise**

PAGE 5

**SIM Swapping:
The Achilles' Heel
of Two-Factor
Authentication**

PAGE 8



Sodinokibi Ransomware: A New Strain Takes the Stage

Through its cyber intake process, Kroll identified 23 ransomware incidents during the month of July 2019 that affected organizations across sectors, including service, retail and education.

Five of the incidents were attributed to Sodinokibi ransomware. Sodinokibi (also known as REvil or Sodin) is a newer ransomware strain that is packaged as ransomware-as-a-service (RaaS), much like its suspected predecessor GandCrab. (See GandCrab Connection discussion in this newsletter.)

Zero-Day Vulnerability Creates an Opportunity for Sodinokibi

According to the [New Jersey Cybersecurity & Communications Integration Cell \(NJCCIC\)](#), one foothold for Sodinokibi ransomware is a known zero-day vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware ([See CVE-2019-2725 Detail in the NIST National Vulnerability Database](#)). The vulnerability allows malware to infect servers without relying on user interaction, as opposed to conventional methods of infection, such as malicious email attachments. Instead, the vulnerability allows attackers to gain access to a server using a web-based connection.

Managed Service Providers Targeted to More Efficiently Monetize Attacks

Another unique attribute of Sodinokibi is its effective use of managed service providers (MSPs) to spread the ransomware. Three of the five Sodinokibi cases Kroll identified in July involved the pushing of the ransomware from another vendor or IT provider into the clients' networks. This is an efficient and effective way for ransomware to reach a large number of victims. In fact, the FBI released an alert in August 2019 noting "multiple U.S. companies suffering infection and encryption of file systems as the result of only one cyber intrusion." MSPs that specialize in serving clients in specific industries, e.g., education or healthcare, can also unwittingly distribute the malware to a large swath of victims in a specific sector.

Associate Managing Director Thomas Brittain notes that many of the affected MSPs have been local or smaller vendors. "In the past, bad actors deploying ransomware were more opportunistic, conducting phishing campaigns hoping to encrypt the recipient. With Sodinokibi, however, cybercriminals are much more targeted, intentional and hands on. For example, in our casework we have seen two levels of reconnaissance in play. Once actors gain access to an MSP, they explore how many clients the MSP serves, the tools that the MSP uses for remote administration and patch management and the level of access in the client's network. If the actors can gain access to the client's network, they conduct a second phase of recon, enumerating the network to determine the total number of systems

as well as any backups for deletion, and finally encrypt the available systems. The actors are then armed with knowledge on the number of clients and systems in each network served by the MSP, enabling them to assess the potential of the MSP or their clients to pay the ransom, usually driving a higher payout.”

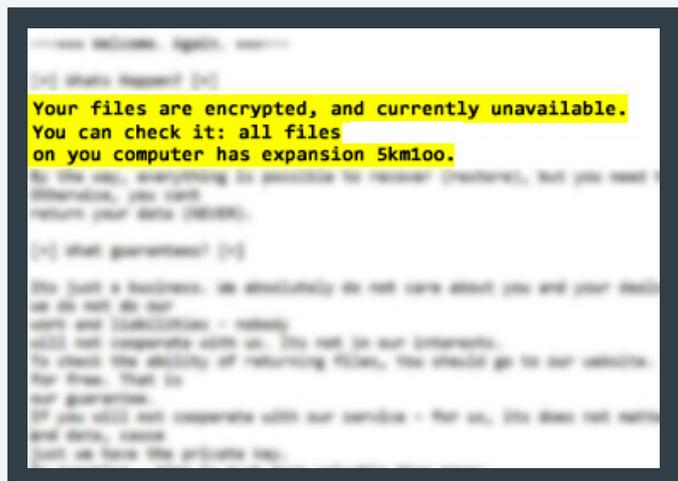


Figure 1 - Example of Sodinokibi Ransom Note

Technically Speaking

The GandCrab Connection

Since appearing on the scene in early 2018, GandCrab is estimated to have cornered a 50% share of the ransomware market at its height and likely affected more than 1.5 million victims globally, according to Europol. A [June 2019 Europol press release](#) described the GandCrab business model:

“Set as a ransomware-as-a-service licensing model, distributors could buy the ransomware on dark web markets and spread it among their victims. In exchange, they would pay 40% of their profit to the GandCrab developers and keep 60% for themselves.”

Sodinokibi ransomware made a splash at the end of May 2019 at the same time GandCrab ransomware brokers purportedly shut down their operations. On May 31, 2019, GandCrab actors

announced their retirement in a dark web post, stating, “We have proved that by doing evil deeds, retribution does not come.”

The timing of these events led incident response teams to speculate that the GandCrab peddlers may have simply tinkered with their ransomware a bit and repackaged it into a new product. For example, according to the NJCCIC, “Some [Sodinokibi] attacks have followed up with an additional attack on the same target, distributing GandCrab v5.2.” The marketing of the variants is similar, and they are both used for RaaS and large-scale attacks.



Figure 2 - Sodinokibi ransomware screenshot

Typical Observed Deployment Pattern

Senior Director Scott Hanson provided the following attributes of Sodinokibi deployment that Kroll has observed in its cases. These techniques are also consistent with [open-source reporting](#):

- Usage of PowerShell to execute the ransomware payload hosted on third-party sites, such as GitHub or Pastebin
 - PowerShell is a native component of the Microsoft Windows operating system used by administrators. For this reason, a malicious PowerShell script is less likely to be blocked than other attacker methods.

- Deletion of volume shadow copies (typical of most ransomware)
 - Volume shadow copies are the result of Windows technology that enable the system to create a snapshot of computer files or volumes while they are in use. Deleting volume shadow copies eliminates a source of backup data for restoring the system.
- Ransom notes have a naming convention of <random alphanumeric>-readme.txt (example in Figure 1)
- Desktop wallpaper image may be changed to a blue image with text including “All of your files are encrypted!” (example in Figure 3)
- Use of PsExec to push the ransomware from an initially compromised system to additional systems on the network
 - PsExec is a command line tool that allows one to execute processes on other systems remotely.



Figure 3 - Sodinokibi ransomware desktop wallpaper

Dark Web Sighting

A post on an open-source website noted the association of the RIG exploit kit with Sodinokibi. Palo Alto Networks defines exploit kit as “automated threats that utilize compromised websites to divert web traffic, scan for vulnerable browser-based applications, and run malware.”

Kroll searched the deep and dark web for references to the RIG exploit kit and discovered a post that advertises the sale of the RIG exploit kit for \$60-\$80 per day (Figure 4).

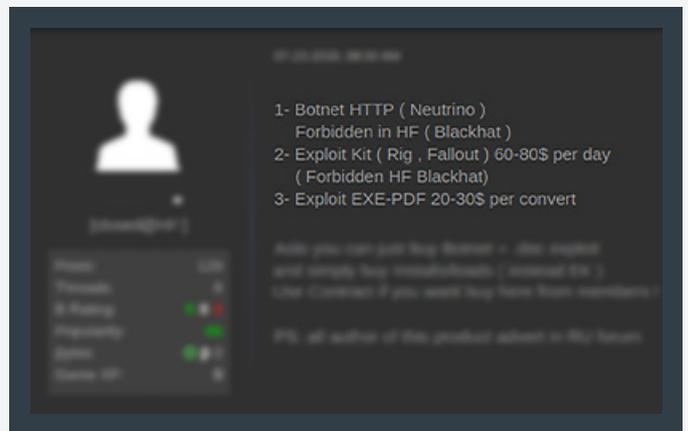


Figure 4 - RIG exploit kit for sale on dark web forum

Case Studies

One incident that Kroll investigated demonstrates an insidious way that Sodinokibi can spread. Kroll's client had remotely connected to one of their servers after realizing their digital surveillance system was not online. They immediately observed unusual text files residing on the desktop in addition to the background displaying a ransom note. A further inquiry revealed all seven of their servers had been encrypted with Sodinokibi ransomware. The affected servers were remotely administered by a third-party digital surveillance company, who alerted the client they had also been infected with the ransomware.



Thomas Brittain
Associate Managing Director

Kroll Experts Corner: Best Practices for Mitigating Sodinokibi

Following are insights from Kroll experts Thomas Brittain, Scott Hanson, Michael Hill and Cole Manaster on how to better defend against Sodinokibi.

- **Patch systems.** Confirm that systems have been patched for the [Oracle WebLogic Server vulnerability](#) that is targeted by Sodinokibi ransomware.
- **Move backups offline.** Offline backups are hard for adversaries to touch. But remember, if your online systems sync to your backups, this provides an avenue for the malware or actor(s) to delete your backups.
- **Monitor remote connections.** Deploy a monitoring solution that can provide visibility on the activity of remote connections and software, such as Remote Desktop Protocol (RDP).
- **Employ 2FA.** Apply two-factor authentication (2FA) to user login credentials and implement least privilege for file, directory and network share permissions.

Key considerations when engaging an MSP

- How is the MSP securing connections to your system?
- Are they leveraging 2FA/MFA for remote connections into your environment?
- What patch management schedule does the MSP follow?
- Will the MSP handle backups and recovery in the event of a ransomware attack?

It's important to have a sound understanding of how an MSP is protecting access to your environment and the full scope of their service offering. This knowledge will enable your team to plan a comprehensive security and disaster recovery strategy that includes securing external network access, patch management, online/offline backups and an incident response plan.

Ransomware on the Rise

From February through the end of August, Kroll investigated over 100 cases of ransomware for clients across diverse industry sectors. Our findings are underscored by a variety of open- and closed-source reporting, including an August 2019 advisory¹ by the Cybersecurity and Infrastructure Security Agency about the “rapid emergence of ransomware across our Nation’s networks.”

In August alone, Kroll observed seven different variants of ransomware, including newer arrivals such as Tflower and DoppelPaymer. Even Ryuk, the ransomware most often detected, has been characterized by multiple different strains and variants.

The increase in variants is making it more difficult for organizations, incident responders and law enforcement to triage ransomware cases. For example, decryptors for new variants may not become publicly available in a timely manner. Likewise, it may take time to produce case studies or anecdotal reporting on how or if threat actors will decrypt the data if the ransom is paid.

Ransomware on the Dark Web

Kroll intelligence analysts conclude that large-scale ransomware campaigns are often carried out by tightknit cyber-criminal groups, such as [Indrik Spider](#), that are motivated by profit. These groups will often operate on their own or are solicited to offer their ransomware as a service (RaaS) to paying customers. As a result, access to these pieces of ransomware is often very restricted and they are not typically offered for sale or for rent on the forums or peer-to-peer chat groups. However, once a group is done with a ransomware campaign, that source code is sometimes leaked, and new pieces of ransomware can be created out of that code.

The result of fewer large ransomware campaigns on forums and peer-to-peer chat applications has been a greater presence of smaller, lesser-known ransomware. Often this malware is developed by small groups or individuals looking to make a name for themselves within this specific community.

One example of this can be found on the top-tier Russian forum Exploit. The ransomware dubbed “Buran” has been offered for sale, with the seller claiming it will work on every version of Windows from XP to 10, encrypt files without changing extensions and delete restore points for the user. It is being sold for a few thousand dollars, and at the time of analysis, it does not appear any user has verified the effectiveness or validity of this specific Buran offering. Interestingly, no one has confirmed whether it is connected to the Buran ransomware strain that is currently reported to be spread via a RIG exploit kit.

buransupport
kilobyte
●●



Paid registration
31 posts
Joined
05/12/19 (ID: 92799)
Activity
other / others

Posted May 13

Buran is a stable offline crypto-fiber with flexible functionality and support 24/7.

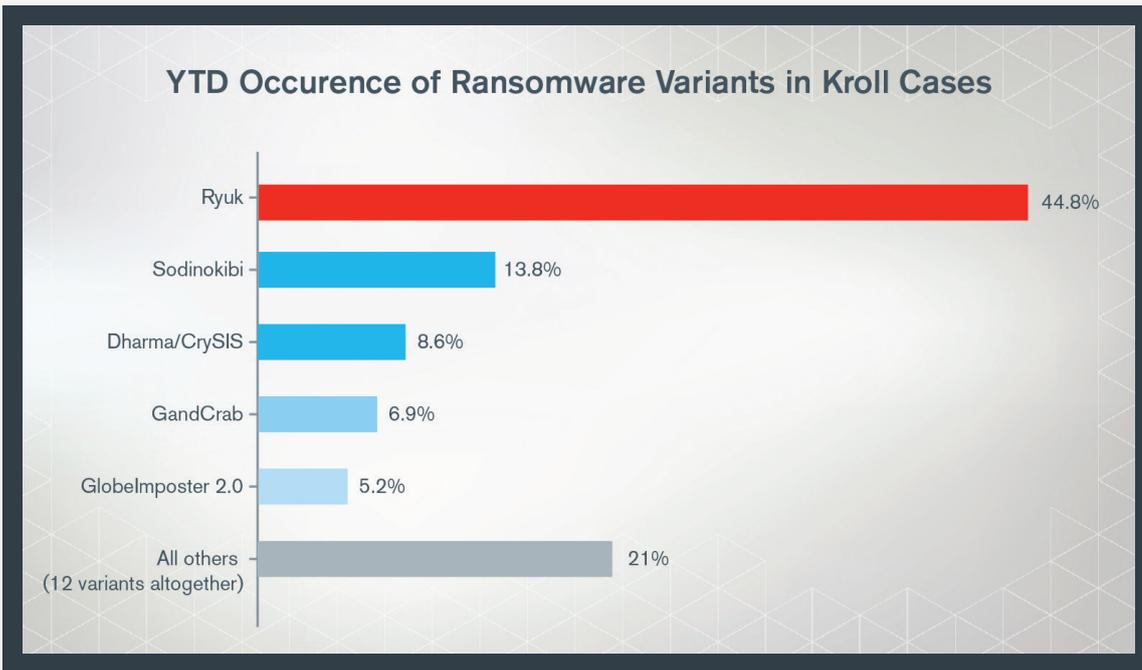
Functional:
Reliable cryptographic algorithm using global and session keys + random file keys;
Scan all local drives and all available network paths;
High speed: a separate stream runs for each drive and network path;
Skipping Windows system directories and browser directories;
Generation of a decoder based on an encrypted file;
Correct work on all operating systems from Windows XP, Server 2003 to the newest;
Loker does not have dependencies, does not use third-party libraries, only math and Winapi
Completion of some processes to release open files (optional, negotiated);
The ability to encrypt files without changing extensions (optional);
Delete restore points + clear logs on a dedicated server (optional);
Standard options: otstuk, autoloop, self-deletion (optional);
Established protection from launch in the CIS segment.

Conditions:
Negotiated individually for each advert, depending on the volume and material.
Start making money with us!

1 - User advertising the “Buran” variant for sale in dark web forum

Ransomware Variants Observed in Kroll Engagements

Below is a list of ransomware (including any related variants) that Kroll has encountered year-to-date in the course of its investigations. Ryuk ransomware accounted for more than triple the number of incidents over the second most common type, Sodinokibi.



The full list includes:

Dharma/CrySIS	Hermes	RobbinHood
DoppelPaymer	Matrix	Ryuk
Evil Locker	Mr.Dec	SamSam
GandCrab	Nozelesn	Snatch
Globelmposter 2.0	Phobos	Sodinokibi
WannaCry		Tflower



Scott Hanson
Associate Managing Director

Kroll Experts Corner:

Best Practices for Ransomware Recovery

Hopefully, your organization will not become a victim of ransomware. However, preparing for the worst-case scenario can help you respond in a quicker, more deliberate manner and limit the impact on your operations. Scott Hanson, a Associate Managing Director in our Cyber Risk practice, recommends that your IT personnel and management team discuss the following best practices now and be ready to implement them quickly in the event you become a victim.

- **Isolate and Disconnect.** If a system within your environment is impacted, isolate it from other computers and servers within the network and disconnect from both wired and wireless networks.
- **Identify the Infection.** Ransomware typically identifies itself within the ransom note. If that is not done, numerous open-source sites such as [No More Ransom](#) and [ID Ransomware](#) may be able to help you identify what variant you have.
- **Report the Incident.** Incidents may be reported by contacting your local FBI field office or through the [FBI Internet Crime Complaint Center](#). Information about ransomware attacks provides law enforcement with better understanding of the scope of the threat and helps them allocate resources toward ransomware research and investigations.
- **Think Before You Pay.** Paying a ransom is ultimately a business decision. Only the victim of a ransomware attack can measure the value of the data loss, the risk to their operations or business and the costs associated with paying versus not paying. Kroll is here to support you in that decision-making process. Whether it is restoring the network from backups or negotiating for a decryptor to restore the business, we can offer our expertise, experience and guidance. Your

incident response plan should outline your stance and response to any cases of ransomware; also, if applicable, contact your [cyber insurance carrier](#) for any ransomware-related coverage.

- **Retain log data.** Preserving network and endpoint logs can make the difference between successful root-cause analysis and being left in the dark as to how the incident occurred. Because many log types roll off quickly, timely action is necessary to retain any potentially relevant event data for subsequent investigation.
- **Restore Systems.** Assuming your backups are still in place, you may choose to wipe your systems altogether and reinstall from safe backups. (For more best practices on backup policies and protocols, see the Kroll Monitor issue, [Ryuk and the Resurgence of Ransomware](#).)

A well-thought-out [incident response plan \(IRP\)](#) is vital if you suffer a ransomware attack. An IRP that is tested on a regular basis will be the “battle plan” that coordinates all the parties enterprise-wide that are necessary to manage a ransomware attack: IT and InfoSec, finance, risk and business continuity, human resources and legal, as well as external partners such as [insurers, legal counsel and investigative or forensics responders](#).

Arranging an incident response retainer with a highly experienced cyber security first responder such as Kroll, can provide additional peace of mind. Kroll offers three incident response retainer plans with no surprises. With our prepaid plans, Kroll lets you customize your retainer with a wide variety of industry-leading reactive and proactive services that ensure you maximize the value of your cyber security investment.

SIM Swapping: The Achilles' Heel of Two-Factor Authentication

Kroll identified a variety of SIM swapping incidents via its intake process for cyber investigations between July and September 2019, two of which resulted in access to victims' financial institutions. Subscriber identity module (SIM)¹ swapping is a type of attack in which a malicious actor induces a mobile service provider to cancel the target's SIM card and then port the target's mobile phone number to the hacker's SIM card and phone. The hacker can then use the hijacked phone number to request SMS-based one-time passcodes² to access the victim's online accounts, reset passwords, or transfer assets.

One of the hallmarks of SIM swapping fraud is the speed of attacks, says Associate Managing Director Pierson Clair. "Hackers don't waste time; once the SIM swap occurs, they immediately start accessing the victim's online accounts, and the financial losses can rack up very quickly," explains Pierson. He notes that beyond traditional financial accounts, any kind of desirable asset is attractive to these cybercriminals, such as cryptocurrency or customer loyalty rewards (e.g., credit card rewards or frequent flyer mileage).

Pierson notes this efficiency is also reflected in the fact that attackers are generally looking to collect readily available public information in order to carry out the swap (see "How Does a SIM Swap Work?" below). Accordingly, people with an extensive public footprint whom an attacker assumes to potentially own assets worth pursuing are favored targets. C-suite executives, business leaders and board members, entrepreneurs, and individuals well known in their industry sector or community often fit the bill perfectly.

Recent Kroll cases and federal indictments indicate a significant trend in targeting individuals involved with cryptocurrency investing and trading. These individuals are increasingly becoming victims because it is easier to leverage SMS-based two-factor verification (2FA) to transfer and launder cryptocurrency accounts compared with traditional fiat currency. (See "In the News" section below.)

While attacks themselves are efficient, unfortunately it can take victims a day or more to figure out what has happened and remediate the damage. Some aspects of a SIM swap attack are out of a person's control (e.g., a network provider employee who mistakenly permits the SIM swap), but Pierson says individuals can proactively take steps to forestall a swap and/or limit damage until they can sort things out with their service provider. These include cybersecurity basics such as avoiding credential reuse across online accounts and taking full advantage of all security features offered by a service provider. Pierson outlines these measures more fully in this newsletter's Experts Corner.

¹. A subscriber identity module (SIM) is a type of smart card that, among other purposes, authenticates the phone's user to the mobile service provider.

². "A one-time passcode or password (OTP) is a code that is valid for only one login session or transaction. An OTP is typically sent via SMS to a mobile phone, and they are frequently used as part of two-factor authentication (2FA)." Source: Idology, <https://www.idology.com>

How Does a SIM Swap Work?

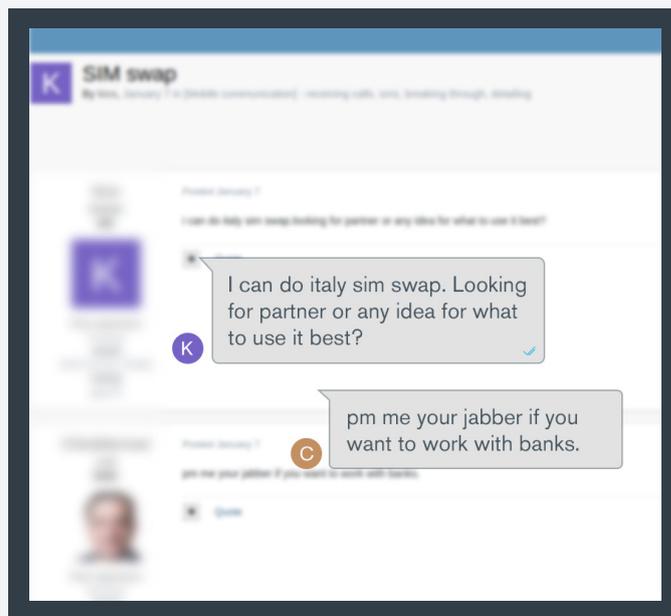
According to Pierson, a SIM swapping attack is primarily a three-step process – identify the target; conduct reconnaissance; then make the swap and drain assets.

- 1. Identify the target.** As mentioned earlier, attackers are looking for high-value targets for whom extensive and accessible data exists. Some of the data can simply be public knowledge (e.g., executives listed on a company's website), but much is commonly shared by victims themselves (e.g., articles, interviews, or postings to various professional and personal social media platforms). Targets with unusual names make it that much easier for attackers to find applicable data faster and avoid false positive results from their research.
- 2. Conduct reconnaissance.** Pierson says the next step for cyberattackers is akin to a background intelligence workup. Drawing on a combination of publicly posted information and dark web sources, bad actors work to glean facts that help with not only the SIM swap, but also later when cracking accounts. For example, if a victim's email addresses and passwords were compromised in a data breach, that information is for sale somewhere on the dark web. A cursory view of social media postings can often provide more than enough clues for guessing usernames and passwords, as well as answers for common account verification questions (mother's maiden name, favorite vacation spot, pet's name, first school, etc.).
- 3. Make the swap and drain assets.** Once a hacker has collected enough information on a target, they will then leverage either social engineering or an insider at the phone company to conduct the SIM swap operation whereby the victim's mobile number is changed to point to the attacker's phone. The attacker can then request one-time passcodes to reset the victim's online accounts, facilitating access to

email, social media, and asset-holding accounts. In cryptocurrency cases, at this point the attacker can transfer crypto assets to a crypto wallet under their control, and then launder cryptocurrencies via various methods available on the dark web.

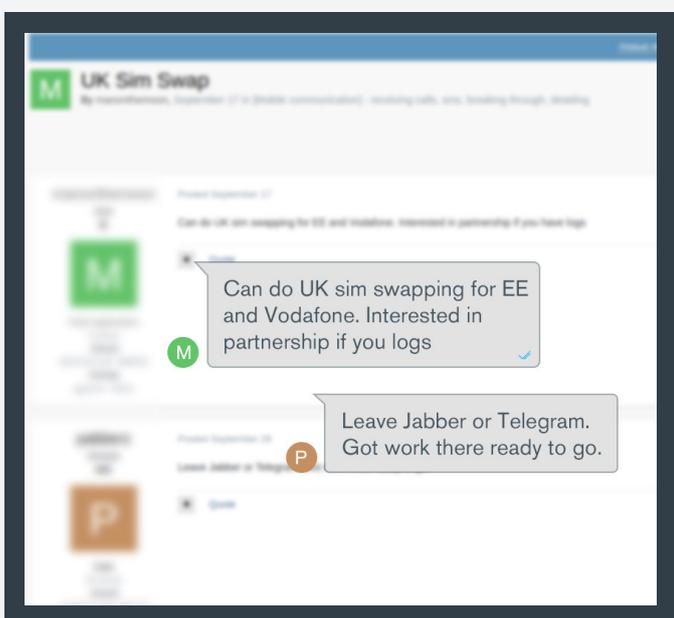
SIM Swapping with Insiders on the Dark Web

Kroll's analysis of dark web marketplaces indicates that there is a large volume of advertisement for SIM swapping services available on multiple forums. In most cases, actors are reluctant to talk about their intentions on the forums and prefer to move to peer-to-peer chat applications, such as Jabber or ICQ. However, based on Kroll's experience, we can assess what these actors are planning or what type of assistance they are seeking. Following are some examples of recent global activity related to SIM swapping.



Example 1 – Actors Looking to Expand Into New Geographies

Kroll assesses that in this exchange, the first actor has the capability to perform SIM swaps for Italian cell providers, but is now looking to expand both geographically and in the types of fraud possible with SIM swapping. A response from another actor insinuates they can help with SIM swaps to bypass two-factor authentication for consumer banking institutions. This post reflects not only the global scope of many SIM swap hackers, but also how actors move to private communication channels after initial contact.



Example 2 – Actors Seeking High-Value Targets

Here we have an actor looking for a partnership with individuals who possess banking logs. They likely have the knowledge to perform SIM swaps, but not enough high-value targets. Banking logs are a hot commodity on the dark web because of the information they contain, such as PII when consumers log in, which in turn can directly lead actors to targets. A response from another actor appears to indicate they have either numbers or bank logs that can swap.

Recent Kroll Engagements Involving SIM Swapping

- A client was targeted with a high volume of spam at the same time the client's phone service was cancelled via a SIM swap attack. On the same day the client's SIM was swapped, an attacker gained access to the company's corporate financial account and attempted to make a transfer.
- A SIM swap event targeted the client's phone just before the telephone company's physical location closed for the evening. This forced the victim to try and report the incident over the phone and prolonged the remediation time period until the victim was able to go to the provider's physical store location when it opened again the following morning.
- Demonstrating the persistence of SIM swap attackers, a client's phone was SIM swapped and appeared to have been quickly remediated within a matter of hours, only to find that one of the victim's email accounts was compromised over one month later (likely by the perpetrators of the original SIM swap attack).





Pierson Clair
Managing Director

Kroll Experts Corner:

Best Practices for Responding to SIM Swapping

Kroll Managing Director Pierson Clair has a few recommendations that can forestall SIM swapping or lessen the overall severity of the attack:

- **Take advantage of additional online account security controls beyond SMS-based 2FA.** Set up additional authentication methods or controls offered by not only your mobile phone service provider, but also the providers of all your other online accounts. These can include the use of PINs, out-of-band authentication, etc. Also, restrict the conditions under which any substantive changes to an account can occur, such as in-person only for mobile phone accounts. Other authentication options include the use of third-party applications (e.g., Google or Microsoft Authenticator).
- **Review your overall online security posture.** Are you a person who has tended to use the same username, password, and security questions across multiple online accounts? If that's the case, Pierson says you have made it that much easier and faster for a SIM swapper to get into your accounts and drain valuable assets. By leveraging different credentials for different accounts, you can potentially slow down an attacker long enough to give yourself the chance to notify account providers and lock down your accounts.

In the unfortunate event you do become a victim of SIM swapping, here are five critical steps you should immediately take according to a recent FBI alert:

- **Report the incident in-person** to your mobile service provider.
- **Access your online accounts** as soon as possible from a secure location or connection and change your passwords.
- **Call your bank(s)** and place an alert on your accounts.
- **Look for unusual activity** over the following weeks and months.
- **Report the incident to the FBI or your local police department.**

Examining Online Exposure for SIM Swapping Vulnerabilities

Successful SIM swapping schemes rely on the cybercriminal's ability to pull together a wide variety of data points on their victims. One way people can gauge their risk (or the risk to leaders in their organization) is through an examination of their data's exposure on both the surface web and the deep and dark web. Associate Managing Director Keith Wojcieszek explains, "Even people who believe they have been very careful sharing information online are often shocked to discover how criminals can connect disparate dots to get the information they need. For example, someone who has never shared their private telephone number online might find it has been listed in a booster club roster for their child's school sports team that another parent posted on a social media site."

Kroll's CyberDetectER® DarkWeb can help examine your organization's and key executives' digital data profile from an attacker's perspective. More importantly, as part of a comprehensive [cyber security risk assessment](#), it enables you to take actions to lessens an attacker's ability to use your data against you.





Contact Us



Keith Wojcieszek

Managing Director, Cyber Risk

keith.wojcieszek@kroll.com | +1 443 295 5082

Based in Washington, D.C., Keith joined Kroll from the United States Secret Service, where he served with distinction for 15 years. Most recently, Keith led the USSS Cyber Intelligence Section, Criminal Investigation Division, where he managed the agency's national response to cyber investigative initiatives focused on protecting the financial infrastructure of the United States. In this role, Keith also coordinated complex international investigations that targeted transnational organized crime networks with an emphasis on cyber and information security.



Nicole Sette

Senior Vice President, Cyber Risk

nicole.sette@kroll.com | +1 609 514 8225

Based in the Secaucus office. Nicole is a highly accomplished security professional, who brings unique insight to the multiple dimensions inherent in client challenges from her years of federal law enforcement and military experience. Nicole served as a Cyber Intelligence Analyst with the Federal Bureau of Investigation for nearly 10 years, and was an Intelligence Specialist with the U.S. Army Communications-Electronics Command for four years.

Browse the latest editions of *The Monitor* and subscribe free at kroll.com/themonitor

About Kroll

Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security and data and information management services. For more information, visit www.kroll.com.

© 2020 Duff & Phelps, LLC. All rights reserved. KR192805

About Duff & Phelps

Duff & Phelps is the global advisor that protects, restores and maximizes value for clients in the areas of valuation, corporate finance, disputes and investigations, cyber security, claims administration and regulatory issues. We work with clients across diverse sectors on matters of good governance and transparency. With Kroll, the leading global provider of risk solutions, and Prime Clerk, the leader in complex business services and claims administration, our firm has nearly 4,000 professionals in 25 countries around the world. For more information, visit www.duffandphelps.com.