



# KNIGHTINK



## RANSOMWARE, INC: THE RISE OF TARGETED RANSOMWARE CRIME SYNDICATES

Revenue generated from cybercrime yields \$1.5 trillion for transnational crime syndicates that goes to funding other illicit criminal activities, such as the global drug and arms trade and human trafficking (Atlas VPN, 2020)

### Summary

This paper discusses the rise of a new threat, targeted ransomware -- or as Microsoft refers to it, "human-operated ransomware." This new type of ransomware is created specifically and fine tuned for the organizations an operator is targeting and is increasingly using "lock and leak" as a tactic to try and increase the number of successful payouts.

### Author Information

Alissa Valentina Knight  
Partner  
Knight Ink  
1980 Festival Plaza Drive  
Suite 300  
Las Vegas, NV 89135  
ak@knightinkmedia.com



**illusive**

### Publication Information

This white paper is sponsored by  
Illusive Networks

Initial Date of Publication:  
December 2020  
Revision: 0.1

# TABLE OF CONTENTS

# 04

- **Key Points**
- **Introduction**

# 11

- **Ransomware Crime Syndicates**
- **Ransomware Gangs**
- **The Business Models**

# 16

- **Ransomware**
- **Tactics and Techniques**
- **Tools**

## TABLE OF CONTENTS

# 24

- **The Rise of the Three Crime Families**
- Big Game Hunters

# 29

- **Solution**
- Solving This New Challenge
- Living off the Land
- Lateral Movement
- Active Defense
- Synthetic Worlds
- Addressing Infrastructure Weakness

# 35

- **Conclusion**
- Summary
- Sources
- About the Author
- About Knight Ink

## KEY POINTS

This section outlines the salient points from this paper. While it's my hope you'll read this paper in its entirety as I couldn't possibly cover every important point this paper makes, this section attempts to summarize the key points.

- Ransomware, which rakes in a cool \$1 Billion per year for its operators, claims a new victim every 11 seconds (Cybersecurity Ventures, 2017).
- Whereas commodity ransomware is employed opportunistically and traditionally got delivered in a "spray and pray" model, operators are now creating targeted ransomware built specifically for the organization they are targeting.
- While one might think the revenues from ransomware and other profit-generating cybercrime would go into frivolous purchases like Lamborghinis and mansions, almost a quarter of revenues generated are reinvested into traditional illicit criminal activities, such as terrorism, human trafficking, and drug production and trade.
- Financial services now represents the 2nd highest number of Ransomware-related breaches across all industries targeted in 2019-2020 (Coveware, 2020)
- Cybercrime syndicates involved in profiting from ransomware must also launder their profits. While money is also laundered through more traditional means, such as through legitimate businesses, ransomware operators are now increasingly turning to laundering their money through cryptocurrencies, like Bitcoin.
- Ransomware crime syndicates, much like the mob that the etymology of the word originated from, have grown from unsophisticated, loosely organized groups of just a hand-full of people. They've now grown in size to become large, transnational criminal enterprises raking in revenues in the billions from operating their own ransomware operations to leasing it out in "ransomware-as-a-service." RaaS affiliate programs adopt a shared revenue model where the operators take a portion of the profits their affiliates generate in a typical 60/40 split (Forbes, 2020).
- The top 3 attack vectors used in the deployment of Ransomware are two predominant tactics, phishing emails and remote desktop protocol (RDP) services opened to the internet. With the COVID-19 pandemic, RDP has increasingly been opened up more so now than ever to employees needing to work from home who still need to access intranet resources for companies.
- Once a ransomware syndicate has established a beachhead on the target network, they deploy a number of tools in support of their tactics, techniques, and procedures (TTPs). No matter what tool is used by the syndicate, pivoting from the initial point of entry or beachhead is a constant indicator of compromise (IoC).

- The idea behind big game hunting is that the syndicates capable of developing their own ransomware or customizing their own fork, create a ransomware payload designed to target a specific organization, industry, or market segment. The threat behind big game hunters is that they typically demand much higher ransom payments, use both lock and leak, and target organizations with much deeper pockets able to afford such payouts.
- After establishing a beach head on the network, syndicates will often as quietly as possible, attempt to escalate privileges if they don't already have them to gain administrative rights over the entire domain so they can pivot around laterally undetected.
- Oft-times, syndicates will use file-less malware as to not disturb disks and file system tables to avoid detection by more sophisticated endpoint detection and response (EDR) and network detection and response (NDR) solutions.
- The most effective method of detection, would be the detection of lateral movement and the effects of living off the land so the syndicates can be identified before the droppers are placed and files encrypted and leaked.
- Living off the land is the concept of a syndicate using already-available tools built into the operating systems in order to achieve their goals rather than downloading and using malicious tools that might otherwise be blacklisted. The increased exodus by ransomware groups from tools like Mimikatz has a lot to do with the syndicates wanting to go undetected for a longer period of time. Whereas tools like Mimikatz might be blacklisted from use in a network and potentially trigger alarms, built-in tools that when combined together can achieve pretty much the same goal are used instead.
- Lateral movement occurs at the second step of a kill chain in a breach. There is no point for a syndicate not to pivot around within a network once the beachhead is established. Lateral movement is a constant, not a variable in a breach. Just like it's said that the only guarantees in life are death and taxes, so can the same be said about lateral movement in a breach.
- Nearly all high-impact cyberattacks have a phase in which the attacker must conduct lateral movement from "patient zero" to the ultimate target. To do this, the attacker needs a combination of credentials and available connections between one system and another. This is the evasive process of "living off the land" using the connectivity native to the organization.

## INTRODUCTION

According to Dr. Michael McGuire, lecturer in criminology at the University of Surrey, revenue generated from cybercrime yields \$1.5 trillion for transnational crime syndicates that goes to funding other illicit criminal activities, such as the global drug and arms trade and human trafficking (Bromium, 2018)

Categorically, ransomware rakes in an average \$1 Billion annually for its operators and claims a new victim every 11 seconds (Cybersecurity Ventures, 2017).

Like drug cartels, crime syndicates involved in the deployment and operation of ransomware take advantage of local government corruption and lack of law enforcement to operate, especially in transit countries, such as eastern Europe and the middle east. These criminal enterprises operate indiscriminately without abandon with little to no concern of intervention by local state or federal authorities.

To ensure they don't anger their own local government, their ransomware programmatically looks for keyboard layouts installed on the target host in their language, such as Russian if operating in Russia, Persian if they're an Iranian group, and so-on. When their own language is detected, the ransomware immediately terminates.

According to Statista, the top three countries operating revenue-generating malware are Belarus, Russia, and Bosnia

and Herzegovina.

However, a new type of ransomware has emerged that is far more sophisticated, customized, and more relevant to the target organization.

This paper was written for cybersecurity engineers and chief information security officers wanting to better understand this new ransomware, colloquially being referred to as targeted ransomware or as Microsoft refers to it, "human-operated ransomware." This new type of ransomware is created specifically and fine tuned for the organizations an operator is targeting and is increasingly using "lock and leak" as a tactic to try and increase the number of successful payouts.

There are two separate types of ransomware gangs, those that use already-developed ransomware-as-a-service (RaaS) tools and those who create their own, targeting specific companies or industry segments. Those who use commodity ransomware as a crime of opportunity, don't need to be sophisticated developers and are being sold as easy-to-deploy, "set it and forget it" crime kits on the dark web. Anyone with or without programming skills can run a network of ransomware infected hosts and generate handsome profits using a RaaS service, such as DarkSide or Sodinokibi among others.

However, this paper focuses on a different type of criminal enterprise, those who create their own ransomware based on the organization or segment they are targeting and demand much higher ransoms on account of their increased level of effort around writing custom code.

Just to put these profits into perspective, the annual revenue generated from the global trade in illegally harvested organs is upwards of \$1.7 Bn (GFI, 2017). The last estimate performed by the United Nations on the revenues generated by the illicit drug trade annually puts it at \$400 Bn. According to a report by the International Labor Organization, the annual revenue for human trafficking is now at \$150 Billion. Even at its most conservative number, this puts the annual revenue generated by cybercrime of \$1.5 Trillion far ahead of the income generated by other criminal enterprises per annum.

While one might think the revenues from ransomware and other profit-generating cybercrime would go into frivolous purchases like Lamborghinis and mansions, almost a quarter of revenues generated are reinvested into traditional illicit criminal activities, such as terrorism, human trafficking, drug production, and the international drug trade.

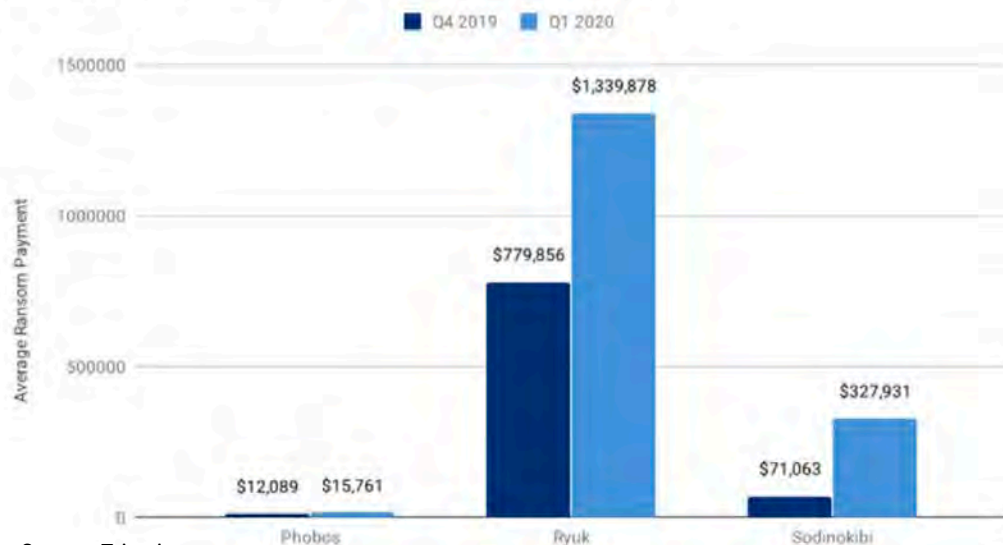
While countless articles, papers, and videos have been created on commodity ransomware, very little is known about targeted ransomware, the operators

running them, their costs, and tactics and techniques used to deploy them. This paper attempts to demystify targeted ransomware and their operators for CISOs and cybersecurity engineers charged with securing their organizations from this new and costly threat.

Simply put, we're in an era now that the world has previously never faced. Whereas commodity malware traditionally got delivered in a "spray and pray" model using phishing and drive-by-downloads, adversaries are now creating targeted malware built specifically for the organizations they are targeting who they estimate will be the most likely to pay.

But unfortunately, true to the metaphor that the temporary wins and losses between adversaries and defenders is a game of cat and mouse, as we make advancements in our tools, so do adversaries.

Average Ransom Payment: Top 3 Ransomware Types



Source: Tripwire

According to research performed by Nationwide Insurance published in August of this year, the average extortion payment made to a ransomware operator by an enterprise due to a ransomware attack was \$111,605 of the 205,280 organizations impacted by ransomware attacks in 2019. The average cost to recover from a ransomware attack now sits at \$84,116, representing a two-times increase from the previous year.

The payouts for even a single ransomware operator, especially if employing targeted ransomware at an organization with deep pockets spells big business for criminals. As an example of just how big the business is, especially for RaaS operators, Gandcrab retired its RaaS service with bragging rights of making its affiliates over \$2 Billion in just over a year of business operations, representing a

gross income for affiliates of \$2.5 Million per week. If the affiliates made \$2 Billion during that period, on an assumed revenue split of 60/40, one can assume Gandcrab grossed roughly \$5 Billion for it's 40% share in revenue in just over a year of operations (Threatpost, 2019).


Affiliates are malicious actors wanting to jump easily and more quickly into becoming a ransomware group by leveraging existing TTPs provided by the RaaS operator that they don't have the resources or capability to develop themselves.



**Gandcrab**

(\ /) \_ (\$ \_ \$) \_ (\ /)

●●●●●●



**Seller:**  
#24 posts  
Joined:  
12/18/17 (ID: 84324)  
Activity  
virology

Posted 18 hours ago

Report post

All the good things come to an end.

For the year of working with us, people have earned more than **\$ 2 billion**, we have become a nominal name in the field of the underground in the direction of crypto-fiber. Earnings with us per week averaged **\$ 2,500,000**.

We personally earned more than **150 million** dollars per year. We successfully cashed this money and legalized it in various spheres of white business both in real life and on the Internet.

We were glad to work with you. But, as it is written above, all good things come to an end.

**We are leaving for a well-deserved retirement**. We have proven that by doing evil deeds, retribution does not come. We proved that in a year you can earn money for a lifetime. We have proved that it is possible to become number one not in our own words, but in recognition of other people.

In this regard, we:

1. Stop the set of adverts;
2. We ask the adverts to suspend the flows;
3. Within 20 days from this date, we ask adverts to monetize their bots by any means;
4. Victims - if you buy, now. Then your data no one will recover. Keys will be deleted.

That's all. The topic will be deleted in a month. Thank you all for the work.

**Source:** Bleeping Computer

Since the retirement of Gandcrab, the affiliates moved to Sodinokibi (Sodin or REvil), which includes its biggest grossing affiliates, Truniger, and Lalartu.

While the sophistication of cybercrime overshadows traditional criminal enterprises, the methods used to launder the money generated from it are roughly the same as your more traditional illicit business models run by drug cartels and human trafficking rings. Like those criminal enterprises, cybercrime syndicates involved in profiting from ransomware must also launder their profits. While money is also laundered through more traditional means, such as through legitimate businesses, ransomware operators are now increasingly turning to laundering their money through cryptocurrencies, like Bitcoin.



KNIGHTINK



# **RANSOMWARE CRIME**

SYNDICATES

## RANSOMWARE GANGS      THE BUSINESS MODELS

The use of the term crime syndicate was first adopted by the media and was defined as a large, loosely connected or close-knit group of gangsters and criminals involved in organized crime. It was historically used to refer to the mafia, originally given to the Italian-American and Jewish mafia connection in the late 19th century.

Ransomware crime syndicates, much like the mob that the etymology of the word originated from, have grown from unsophisticated, loosely organized groups of just a hand-full of people. They've now grown in size to become large, transnational criminal enterprises raking in revenues in the billions from operating their own ransomware operations to leasing it out in "ransomware-as-a-service." RaaS affiliate programs adopt a shared revenue model where the operators take a portion of the profits their affiliates generate in a typical 60/40 split (Forbes, 2020).

There are four prolific actors in the cyber crime syndicate underworld among the thousands, if not more, players. The more notable include Maze (now defunct), Ryuk, Phobos, and Sodinokibi.

While these groups historically relied on other dark web marketplaces to sell their leaks, they've now begun to cut out the middlemen and began deploying their own dedicated marketplaces to hawk their wares.

There are different business models adopted by these syndicates in how they generate revenue. Some of the ransomware has a single developer and maintainer, and some have forked off into new ransomware variants with no single individual or group maintaining it. Where there is a single developer and maintainer of the codebase, such as Pinchy Spider, Indrik Spider, Wizard Spider, and so-on, I've identified them here. The second name given to each syndicate of "Spider" was established and given to them by CrowdStrike's intelligence group who tracks and monitors them. The name Spider is given to any group involved in eCrime.

Groups generate their revenue off of the use of their own ransomware, such as Indrik Spider with Bitpaymer. That group will then profit off its network of affiliates in a common revenue sharing model of 60/40, with 40% going to the group and 60% going to the affiliate. The group will also sell RDP credentials it has harvested from victim networks, giving it a potential of 3 separate revenue streams, which is how groups like Gandcrab were able to start and then retire as billionaires in just 16 months of operations.

Presented here are two parent categories of RaaS and Non-RaaS groups, then further broken down by the syndicate's modus operandi for generating income through lock, leak, or both lock-and-leak.

With the ability for groups to profit from the use of their own ransomware and profit from revenue sharing with affiliates by starting a RaaS, very few groups now operate independently without running a RaaS service.

Similarly, as lock-and-leak compels more organizations to pay extortions, groups who previously just locked or leaked are now increasingly moving to a lock-and-leak model in order to better guarantee payments.

**Ransomware-as-a-Service (RaaS):** RaaS services offer their ransomware as a tool to affiliates. Affiliates often split their payouts with the RaaS operator in a 60/40 split (Forbes, 2020), with the affiliates taking 60% of the profit and the rest going to the RaaS operator. Once they reach 3 successful extortion payments, the affiliate is often bumped up to a higher percentage to 70%. The RaaS operator offers quite a sophisticated toolset for its affiliates, including the luxury of an administrator dashboard and a dedicated site where dumps (stolen data) can be automatically published if a victim refuses to pay.

The affiliates can even outsource different parts of the attack, including techniques like RDP brute forcing. Some of the more recognized and active RaaS services include:

- Avaddon (Lock & Leak)
- CLOP (Lock & Leak)
- Conti (Lock & Leak)
- Maze (Defunct)
- Phobos, Lock
- Sodinokibi (REvil) (Lock & Leak)
- Darkside (Lock & Leak)
- Doppelpaymer (Lock & Leak)
- Ryuk (Lock & Leak)
- Netwalker (Lock & Leak)
- Ranzy (Lock & Leak)





KNIGHTINK





# **RANSOMWARE**

TACTICS, TECHNIQUES, AND PROCEDURES



## Tactics, Techniques, and Procedures

The top 3 attack vectors used in the deployment of Ransomware are two predominant tactics, phishing emails and remote desktop protocol (RDP) services opened to the internet. With the COVID-19 pandemic, RDP has increasingly been opened up more so now than ever to employees needing to work from home who still need to access intranet resources for companies. Had these companies implemented secure remote access using solutions, such as virtual private networks (VPNs), perhaps they wouldn't have fallen victim to these ransomware attacks—at least not using RDP as a point of entry.

Therefore, detection of lateral movement is key to identifying the ransomware syndicate in the network as quickly as possible before the droppers are placed on endpoints. This is commonly referred to as lowering mean-time-to-detection (MTTD) and mean-time-to-response (MTTR).

I should clarify that not all of these tools are malicious. Many of the tools listed here were created and even acquired by Microsoft as system administration tools for server admins. They simply provide a utility needed by the syndicates to more quickly and easily achieve their actions on objectives.

## Tools

Once a ransomware syndicate has established a beachhead on the target network, they deploy a number of tools in support of their TTPs. No matter what tool is used by the syndicate, pivoting from the initial point of entry or beachhead is a constant indicator of compromise (IoC).

Many groups, especially those using targeted ransomware like SamSam or Ryuk are also going after and encrypting the victim's backups making restoration of backups impossible. In order to do this, pivoting (also known as lateral movement) is also necessary as the group "lives off the land" and learns what data is being stored, where it's being stored, and how it's being stored.

**Masscan** was developed by Robert Graham and is the fastest port scanner in existence, capable of scanning the entire internet in just under 6 minutes by transmitting 10 million packets per second using its own custom TCP stack.

**NLBrute (AKA nl.exe or nlbrute.exe)** was created by a Russian developer for brute forcing Windows credentials over remote desktop protocol (RDP). NLBrute can be fed with a dictionary list/word file for the brute force efforts, or a list of passwords from previous credential dumps also referred to as “credential stuffing.”

**Mimikatz:** Often cited as one of the most fundamental contributions to cybersecurity in the last two decades, demonstrates vulnerabilities in Microsoft’s authentication protocols by allowing those who run it to dump credentials, even Kerberos tickets from the system to steal authentication credentials as well as escalate privileges. Mimikatz was developed by Benjamin Delpy and has been integrated into numerous penetration testing platforms as the de-facto standard for post-exploitation techniques, such as Rapid7’s Metasploit. Ransomware syndicates often use Mimikatz to grab credentials from the system’s LSASS process they establish a shell on as they pivot around within the network until an account with Domain Administrator or Enterprise Administrator privileges are discovered.

**Everything.exe:** Everything is another innocuous tool created for system administration and was originally meant for administrative purposes for those managing a Windows domain. Everything is arguably the fastest tool available for searching an entire Windows domain for specific files, such as performing keyword searches for, well, pretty much everything. Ransomware syndicates will use Everything to perform keyword searches across hosts for passwords, social security numbers, or credit card numbers.

**Cryptojacking:** Many Ransomware droppers will also drop cryptomining software allowing the syndicate to use the computational power of target systems to mine cryptocurrency. Cryptojacking is the unauthorized use of a victim’s GPU or CPU to mine cryptocurrency. Many cryptomining scripts have worming capabilities allowing it to self-propagate to other hosts, turning those new hosts into cryptominers as well. Some of the malicious cryptojacking tools used by syndicates include Minergate, Graboid, and Badshell. Which cryptojacking tool is used is inconsequential and will differ by group.

However, the important takeaway here is that syndicates are adding yet another line of revenue to their campaigns. If they are successful in adding a block to the end of the Bitcoin ledger using mining, their profit on top of any extortion payments made and from the sale of the stolen data or credentials on the dark web, can be compounded by the mining award of 12.5 Bitcoins for cryptojacking the organization's hosts. If successful, this nets the group an additional \$237,500 USD at the current Bitcoin-USD price of \$19,000.

**RDP Brute (z668)** is similar to NL Brute in that it is a high-performance brute force utility for Active Directory domains.

**LaZagne** is a free, opensource Github project designed to dump passwords for different applications on the host, such as passwords for web sites stored in web browsers and other applications, such as Skype and Outlook.

**Qwinsta** is short-hand for "query session" and is a built-in command-line utility for querying sessions on Terminal servers or a Remote Desktop Session Host (RD Session Host). Syndicates will use Qwinsta to query active RDP sessions for logged in users and systems they are targeting.

**ProcDump** is similar to Mimikatz, ProCDump is used to dump credentials out of the LSASS process on Windows systems. ProCDump was part of the sysinternals suite of tools, later acquired

by Microsoft.

**PsExec** is another utility part of the old sysinternals suite of tools, PsExec allows an administrator to remotely execute binaries on Windows systems.

**Cobalt Strike (cracked)** is a commercial-off-the-shelf (COTS) solution sold by Strategic Cyber, LLC that provides penetration testers a Swiss Army Knife of functionality for adversarial simulation and red teaming.

Cobalt provides a fileless, multi-stage agent it calls beacons that don't install or touch the victim host's file system and hard disk allowing it to go undetected by most antimalware solutions. The beacons stack multiple utilities in a single agent, including Mimikatz, key logging, SOCKS proxy, persistent backdoor access, privilege escalation, and more. A cracked version of Cobalt Strike is increasingly being used by syndicates and is available for sale on many market places.

**csvde.exe** is a built-in Windows command line utility capable of importing and exporting data into a comma-separated values (CSV) file. Csvde is used by syndicates to dump user accounts, systems (endpoints), and applications in the AD forest with little to no detection than more noisy AD cracking tools to find target hosts to deploy ransomware droppers/payloads to.

**Powershell Empire** is a post-exploitation agent designed to allow penetration testers to use tools typical to the post-exploitation stage of an established beach head on a network enabling encrypted communication, lateral movement, keystroke logging, and credential harvesting without having to use Powershell.exe.





KNIGHTINK





KNIGHTINK



# RISE OF THE THREE

CRIME FAMILIES



## BIG GAME HUNTERS

This new version of ransomware and their syndicates have been referred to using three different names, targeted ransomware, human operated ransomware, and big game hunters. For purposes of this paper, I'll use big game hunters as the term to refer to the syndicates behind creating ransomware aimed at specific organizations or target market segments I'll call targeted ransomware. Targeted ransomware is typically not found for sale in the market places and are held closely by their respective syndicates and their affiliates.

The idea behind big game hunting is that the syndicates capable of developing their own ransomware or customizing their own fork, create a ransomware payload designed to target a specific organization, industry, or market segment. The threat behind big game hunters is that they typically demand much higher ransom payments, use both lock and leak, and target organizations with much deeper pockets able to afford such payouts.

While any syndicate can turn targeted, very few have the development skills to do it. There are currently just a handful of big game hunters that have been identified and are actively being tracked. These syndicates include Boss Spider, Indrik Spider, and Wizard Spider who run the Samas (SamSam), Bitpaymer, and Ryuk ransomware families respectively.

### **Boss Spider**

Boss Spider is credited with the launch of the SamSam (AKA Samas) ransomware, targeting businesses rather than

individuals in order to demand higher payouts. Adopting the lateral movement techniques of state sponsored actors, Boss Spider locates the domain controller, then finally encrypts the organization's data.

#### **Ransomware Profile:**

- Name: Samas
- Companies/Sectors Targeted: Healthcare, government, education, and businesses
- Profits: Between 2016-2018, \$6.4 Million
- Techniques: Samas typically exploits JBOSS using the open source JexBoss toolkit or uses more traditional techniques of RDP brute forcing

### **Indrik Spider (AKA Evil Corp)**

Indrik Spider historically focused on bank wire fraud and after seeing how much easier it was for Boss Spider to monetize its breaches without having to use extensive money laundering mule networks, it switched tactics and thus was born Bitpaymer. The group leveraged its previously created malware, Dridex to drop Bitpaymer ransomware payloads on the victim's network where it then moves laterally deeper into the network.

#### **Ransomware Profile:**

- Name: Bitpaymer
- Companies/Sectors Targeted: Any small to middle-sized organization is a target, this includes industries like finance, agriculture, and technology
- Profits: \$1.5M USD in the first 15 months of ransomware operations.
- Techniques: Phishing payload downloads and executes Dridex, which drops Bitpaymer on the host.

**Wizard Spider**

Wizard Spider (FKA Grim Spider) is a Russian syndicate known for originally developing and operating the Trickbot banking malware. It has since expanded its malware portfolio to include Ryuk, Conti, and Bazerloader.

**Ransomware Profile:**

- Name: Ryuk
- Companies/Sectors Targeted: Business, healthcare, government
- Profits: Between February 2018 to October 2019, \$61 Million
- Techniques: The group uses Trickbot and Bazerloader for initial ingress into the network, then using Ryuk and Conti as the ransomware payloads to lock discovered data in the network. The group originally used Ryuk as its initial ransomware payload but slowly began migrating its network to its newer payload, Conti.





KNIGHTINK



# SOLUTION

WHAT TO DO

## SOLVING THIS NEW CHALLENGE

"Proactive measures, strong monitoring and a clear policy of not paying is imperative." –Bank Info Security

Like everything in cybersecurity, monitoring for specific tools or exploits is ineffectual. Just like the U.S. military doesn't identify enemies just by the firearms or bullets they use. Tools and exploits change and constantly evolve, as do the signatures they create in packet payloads on the network. Therefore, the most effective approach to lowering MTTD and MTTR is monitoring for the constants — the TTPs that rarely change with new tools and exploits.

The constant in the majority of ransomware breaches is lateral movement where the adversary pivoted from their initial beachhead on the network to other endpoints in the network where tools were then used to harvest credentials, create or modify privileged accounts, group policies (GPOs), Windows registries, running tasks, and services configured to start at startup.

Therefore, an effective method of detection, would be the detection of lateral movement and the effects of living off the land so the syndicates can be identified before the droppers are placed and files encrypted and leaked.

if they don't already have them to gain administrative rights over the entire domain so they can pivot around laterally undetected.

Oftentimes, syndicates will use file-less malware as to not disturb disks and file system tables to avoid detection by more sophisticated endpoint detection and response (EDR) and network detection and response (NDR) solutions.

They'll also use command line tools built into the operating system itself, using these built-in tools against the systems, such as Powershell and WMI to better understand where they've landed in the network and what level of privilege they have using these tools for reconnaissance.

## LIVING OFF THE LAND

After establishing a beach head on the network, syndicates will often as quietly as possible, attempt to escalate privileges

Living off the land is the concept of a syndicate using already-available tools built into the operating systems in order to achieve their goals rather than downloading and using malicious tools that might otherwise be blacklisted. The increased exodus from tools like Mimikatz has a lot to do with the syndicates wanting to go undetected for a longer period of time. Whereas tools like Mimikatz might be blacklisted from use in a network and potentially trigger alarms, built-in tools that when combined together can achieve pretty much the same goal are used instead.

## LATERAL MOVEMENT

Lateral movement occurs at the second step of a kill chain in a breach. There is no point for a syndicate not to pivot around within a network once the beachhead is established. Lateral movement is a constant, not a variable in a breach. Just like it's said that the only guarantees in life are death and taxes, so can the same be said about lateral movement in a breach.

As discussed earlier, the first step in lateral movement for the syndicate is to use tools such as LaZarus or Mimikatz to dump credentials from the system they've established a beachhead on.

Once those credentials are gained, queries are performed to determine whether any of those credentials or Kerberos tickets have domain administrator or enterprise administrator privileges. The syndicate will move laterally within the network until a system is reached that contains domain

admin or enterprise admin credentials from a credential or ticket dump on a host. Once achieved, the syndicate will oft-times dump information from the AD server in order to ascertain high value targets within the environment, dump other credentials, and in general, get a better understanding of the environment in which they'll live off until the objectives have been met. Primarily, the group will exfiltrate stolen data, then encrypt it in hopes of a ransom payout.

Powershell Empire enables syndicates to more easily navigate their way laterally around a victim's environment using pass-the-hash, WMI, PsExec, and PsRemoting.

## ACTIVE DEFENSE

MITRE Shield is a new matrix of tactics, techniques, and procedures designed for defenders in how to instrument their network for an active defense security posture. Shield is the product of ten years of MITRE's analysis into adversarial maneuvers taken against their own networks ranging from basic cyber defensive capabilities to cyber deception and adversary engagement.

The premise behind Shield is to arm defenders with a new concept of active defense by employing limited offensive actions and counterattacks to deny their network and its assets to adversaries. While the abstraction of active defense is a novel idea in cybersecurity, it isn't new in military operations.

In summary, Shield is a matrix of tactics, techniques, and procedures for defenders and has since been coupled with MITRE ATT&CK to form a more complete picture between adversarial tactics and techniques and those applied by defenders in their mapped opportunity space.

Deception technology is relied upon heavily in the new Shield matrix for organizations that if adopted, can more effectively and quickly detect lateral movement within an environment once the ransomware loader or beach head is established.

## SYNTHETIC WORLDS

Deception technology is a relatively new product space of security controls capable of creating a high-fidelity detection system using breadcrumbs to bait adversaries away from real, production systems in order to decrease the MTTD by identifying their lateral movement in a synthetic environment created with decoys.

Up until just recently, it was difficult for chief information security officers (CISOs) to understand where in their budget deception technology fit -- where in their security control framework it sits. They simply didn't know whether it's a need to have or nice to have in their arsenal.

MITRE Shield has made it clear that deception technology is now a business imperative with today's reality of "when" advanced ransomware or an adversary will establish a beachhead rather than "if." In 2020, prevention is no longer a realistic goal, leaving CISOs to try and lower the amount of time it takes to detect the adversary once a breach occurs.

Deception technology is now being adopted to improve early detection and deterrence, identifying the technique used by adversaries, which is pivoting/lateral movement.



Much of the tactics defined in Shield are achieved using deception technology, to include decoy accounts, decoy content, decoy credentials, decoy networks, decoy personas, decoy processes, decoy systems, and decoy diversity.

By creating this synthetic environment for syndicates once they've established their beachhead allows them to interact with realistic-looking credentials and assets. Deception technology gives early notice to the organization that they've been breached while keeping the syndicates away from production systems. Using deception technology also allows organizations to shrink the real attack surface while increasing a synthetic attack surface for the syndicates to interact with, also referred to as attack surface management.

## Addressing Infrastructure Weakness

Infrastructure weakness allows syndicates to breach edge defenses in order to establish a beach head in the network environment through weak protocols, such as RDP and SMB, and other software vulnerabilities that create a network ingress point.

Once established, syndicates pivot around within the environment without network controls preventing lateral movement to endpoints that should have been segmented into more secure enclaves of the environment.



KNIGHTINK



# CONCLUSION

AUTHOR'S FINAL  
THOUGHTS

## SUMMARY

Organizations need a well-formed defensive strategy against ransomware that includes good cybersecurity hygiene, such as a documented and regularly updated patch and vulnerability management program, routine annual risk assessments, regular penetration tests, and a regularly updated and maintained asset management system.

Indispensable to any cybersecurity program is a solution that is capable of leveraging deception to detect lateral movement early and capable of deploying decoy accounts, content, credentials, networks, personas, processes, and systems.

In addition to being able to effectively and quickly detect lateral movement, the ability to manage your attack surface should also be inherent to your layered defense model so that the attack surface is reduced to a manageable level. After all, you can't protect what you don't know you have.

The attack surface management capability should be able to automatically discover and map the environment and its "crown jewel" assets and the attack path to get there, identification of conditions exploited for lateral movement, and the ability to find shadow admin accounts, local admins, domain user credentials, and saved connections to the crown jewel assets discovered.

Deception technology should be used with caution. Many of the deception solutions on the market are agent-based and can be easy to identify, making it clear to the adversary that they are in a synthetic environment created by decoys.

The deception technology used should ideally be agent-less and able to self-destruct to eliminate any traces of itself to limit the evidence of any synthetic environment being created.

## SOURCES

Cybersecurity Ventures. (2017). Global Ransomware Damage Costs Predicted To Reach \$20 Billion (USD) By 2021. <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/>

McGuire, M. M. (2018, April 21). The Web of Profit: A look at the cybercrime economy. VentureBeat. <https://venturebeat.com/2018/04/21/the-web-of-profit-a-look-at-the-cybercrime-economy/>

Arežina, L. (2020, November 29). Ransomware statistics in 2020: From random barrages to targeted hits. DataProt. <https://dataprot.net/statistics/ransomware-statistics/#keyransomwarestatistics>

Human Rights First. (2017, January 7). Human Trafficking by the Numbers. <https://www.humanrightsfirst.org/resource/human-trafficking-numbers>

Worldometer. (2020, January 1–December 13). Drug Statistics [Spending on illegal drugs this year]. <https://www.worldometers.info/drugs/>

Nationwide Insurance: <https://www.nationwide.com/cps/cic/blog/cost-of-ransomware-attacks.html>

Schwartz, M. J. S. (2019, November 4). Ransomware Gangs' Not-So-Secret Attack Vector: RDP Exploits. Bank Info Security. <https://www.bankinfosecurity.com/ransomware-gangs-not-so-secret-attack-vector-rdp-exploits-a-13342>

Schwartz, M. J. S. (2020, April 30). Ransomware: Average Business Payout Surges to \$111,605. Bank Info Security. <https://www.bankinfosecurity.com/ransomware-average-business-payout-surges-to-111605-a-14205>

Frankoff, S. F., & Bex Hartley, B. H. (2018, November 14). Big Game Hunting: The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware. CrowdStrike. <https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/>

Loui, E. L., Scheuerman, K. S., Pickett, A. P., & Feeley, B. F. (2020, April 16). Dharma Ransomware Intrusions Exhibit Consistent Techniques. CrowdStrike. <https://www.crowdstrike.com/blog/targeted-dharma-ransomware-intrusions-exhibit-consistent-techniques/>

CrowdStrike. (2020). 2020 Global Threat Report. <https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf>

Microsoft Threat Protection Intelligence Team. (2020, March 5). Human-operated ransomware attacks: A preventable disaster. Microsoft.  
<https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>

Cobalt Strike (Malware Family). (2020, December 13). In Malpedia.  
[https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt\\_strike](https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike)

The CrowdStrike Intel Team. (2020, October 24). Ransomware + Data Leak Extortion: Origins and Adversaries, Pt. 1. Crowdstrike.  
<https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/>

Cyware Hacker News. (2020, March 4). This is How Much Operators of Prominent Ransomware Made in Last Six Years | Cyware Hacker News. Cyware.  
<https://cyware.com/news/this-is-how-much-operators-of-prominent-ransomware-made-in-last-six-years-705edc88>

The CrowdStrike Intel Team. (2020a, October 16). Wizard Spider Modifies and Expands Toolset [Adversary Update]. Crowdstrike. <https://www.crowdstrike.com/blog/wizard-spider-adversary-update/>

Constantin, L. (2020, May 12). Ryuk ransomware explained: A targeted, devastatingly effective attack. CSO Online. <https://www.csoonline.com/article/3541810/ryuk-ransomware-explained-a-targeted-devastatingly-effective-attack.html>

Atlas VPN. (2020, March 11). Cybercrime annual revenue is 3 times bigger than Walmart's. <https://atlasvpn.com/blog/cybercrime-annual-revenue-is-3-times-bigger-than-walmarts/>

Vamosi, R. (2020, November 27). The Emerging Ransomware-As-A-Service Economy. Forbes. <https://www.forbes.com/sites/robertvamosi/2020/11/27/the-emerging-ransomware-as-a-service-economy/?sh=9ff2bc274500>

McGuire, D. M. (2018, April). Into the Web of Profit. Bromium.  
[https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit\\_Bromium.pdf](https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf)



KNIGHTINK



## ABOUT THE AUTHOR

Alissa Knight is a partner at Knight Ink and blends influencer marketing, content creation in writing and video production, go-to market strategies, and strategic planning for telling brand stories at scale in cybersecurity.

She achieves this through ideation to execution of content strategy, storytelling, and execution of influencer marketing strategies that take cybersecurity buyers through a brand's custom curated journey to attract and retain them as long-term partners.

Alissa is a published author, having published the first book on hacking connected cars and am working on a new series of books into hacking and securing APIs and microservices.



## ABOUT KNIGHT INK

### **Firm Overview**

Knight Ink is a content strategy, creation, and influencer marketing agency founded for category leaders and challenger brands in cybersecurity to fill current gaps in content and community management. We help vendors create and distribute their stories to the market in the form of written and visual storytelling drawn from 20+ years of experience working with global brands in cybersecurity. Knight Ink balances pragmatism with thought leadership and community management that amplifies a brand's reach, breeds customer delight and loyalty, and delivers creative experiences in written and visual content in cybersecurity.

Amid a sea of monotony, we help cybersecurity vendors unfurl, ascertain, and unfetter truly distinct positioning that drives accretive growth through amplified reach and customer loyalty using written and visual experiences.

Knight Ink delivers written and visual content through a blue ocean strategy tailored to specific brands. Whether it's a firewall, network threat analytics solutions, endpoint detection and response, or any other technology, every brand must swim out of a red sea of competition clawing at each other for market share using commoditized features. We help our clients navigate to blue ocean where the lowest price or most features don't matter.

We work with our customers to create a content strategy built around their blue ocean then perform the tactical steps necessary to execute on that strategy through the creation of written and visual content assets unique to the company and its story for the individual customer personas created in the strategy setting.

### **Contact Us**

Web: [www.knightinkmedia.com](http://www.knightinkmedia.com)

Phone: (702) 637-8297

Address: 1980 Festival Plaza Drive, Suite 300, Las Vegas, NV 89135



