Prepared Written Testimony of Bill Siegel, CEO and Co-Founder of Coveware Inc.

Federal Spending Oversight Subcommittee of the Committee on Homeland Security and Governmental Affairs

State and Local Cybersecurity: Defending Our Communities from Cyber Threats Amid COVID-19

Wednesday, December 2nd 2020

Table of Contents:

Background on Coveware

Coveware is a boutique cyber incident response firm that focuses on helping organizations and enterprises through cyber extortion events. Since founding in 2018, Coveware has handled over 2,000 cyber extortion incidents, the majority of which have involved ransomware. The firm's main area of expertise is focused on negotiating with threat actors on behalf of our clients that face extortion demands, and navigating the technicalities of restoring data that has become encrypted. We work alongside privacy attorneys, forensic investigators, restoration firms, and cyber insurance companies and are a member of the No More Ransom Project. Our position during these incidents has provided us with a perspective which has shaped our opinion on ransomware and how to reduce the prevalence of it.

One of the central ways that we aim to fix this problem is through the collection of data. In order to solve any large problem, we first need to understand the facts. With ransomware, there are very few static pools of hard data collected first hand from actual incidents. One of the central reasons we founded Coveware was to change this. We collect a large cohort of data from every case we manage. The data exhausted from the incidents we manage is used for 3 principal activities:

1. To build reporting and analytics that help us navigate future incidents on behalf of our clients.
2. To publish research and reporting about the trends and patterns of cyber extortion attacks, so that readers can learn and hopefully secure their networks.
3. To assist law enforcement investigations of these crimes. We provide law enforcement agencies (principally in the U.S. but also abroad) with a flat file of hard data each quarter. This data augments active investigation into the criminal groups that carry out these attacks.

There are actually a surprisingly small group of ransomware actors that are active at any given time (see Appendix A). Year over year, the composition can change, but week over week, it is typically no more than a dozen variants or groups. These groups use the same repetitive tactics over and over again on successive victims. Why the repetition? If it works and is profitable, there is no reason to change. These are economically rational behavioral traits.

Profile of a Typical Ransomware Attack

A typical ransomware attack involves three distinct phases:

1. **Gaining persistence:** A threat actor gains access to the network of an organization. There are several common vectors through which persistence on the network is

achieved (to be discussed later). Regardless of the means by which access is achieved, threat actors will typically elevate themselves to administrative user privileges, allowing them to move freely through the network and control critical systems like domain controllers, anti-virus protection, endpoint protection, authentication, and the back-up systems. During this phase, the actor may attempt to steal banking passwords (so they can be monetized separately) and exfiltrate sensitive data (for further sale to third parties or to add leverage in the extortion). They will map the network and develop a plan to encrypt it.

2. **Detonation:** After sufficient time surveilling and exfiltrating data, the last step is the detonation of the ransomware. The threat actors will turn off antivirus and endpoint protection, which essentially cuts the alarms that would otherwise alert the company. They will delete or encrypt the organization's backup systems. This cripples the company's ability to restore their network quickly. Finally the threat actors will fully encrypt the primary servers and computers of the company. Once the encryption is finished, ransom notes are left on every machine of the organization. They then wait to be contacted.
3. **Extortion:** If the organization has not properly segmented or air gapped their backups, they are effectively crippled. The organization's email is likely inoperable. Their website may be down. Enterprise Resource Planning application systems that control billing, payroll, shipping and other critical functions may be crippled, and phone systems may also be down. Most organizations have to resort to some form of paper and pencil operations if they are truly crippled to this extent. If the degree of interruption threatens the viability of the company, they face two terrible choices: i) choose to lose their customers, dismiss their employees and possibly close their company, or ii) negotiate and pay the ransom demanded by the threat actors. This is the exact choice thousands of organizations are faced with every year. When victims choose to pay a ransom in cryptocurrency to the threat actor, the threat actor may provide a decryption key, though the efficacy of the decryption key can vary between threat actor groups as does the likelihood of receiving the key.

A larger schematic of a typical ransomware attack is provided in Appendix B.

Background on the Cyber Extortion Industry

The common perception of these attacks is that victims are the *targets* of individual threat actors. Coveware believes this is a dangerous misconception, and that resetting this perception is a fundamental step towards becoming safer. We believe that every computer, on every network that is connected to the internet is a target. The only thing that determines who actually gets targeted and attacked is the relative economics between comparable targets.

Financially motivated cyber criminals run their own operations like businesses. Their operations coordinate and transact with other specialized groups within the cyber extortion industry just like in any other legitimate industry or market. The groups that conduct ransomware attacks are separate and unique from groups that perform other critical functions. Some groups focus further up the supply chain and are more akin to raw materials producers. These groups actually construct the malware and ransomware code, but don't carry out attacks. There are other groups that specialize in gaining access or persistence. These groups collect stolen credentials, which they then sell to other groups. There are groups that specialize in running elicit dark marketplaces or forums. These forums serve as trading, logistics and communications outposts. The moderators of these forums can serve as escrow agents for goods and payments, and also enforce rules or resolve disputes. There are groups that specialize in the exfiltration and storage of data. Other groups specialize solely in the deployment of ransomware and extortion. Lastly, there are groups that specialize solely in the cash-out process and laundering of extortion proceeds.

All of these components work together cohesively. The industry is globally distributed, well financed and highly profitable. As we can see, this industry has all the trappings of a mainstream legitimate industry. There are raw materials, refined materials, distribution, logistics, finance, communications, and rules. Reputation also matters greatly in this industry even though its participants are largely anonymous to each other. Also, like any other for-profit industry, economics matter. We make this point because in our experience, the power laws of economics tend to be the most effective way to influence the direction of the industry. Active prevention and aggressive pursuit of criminals by law enforcement will never have substitutes, but are dependent on resources. Applying pressure to the economics of the cyber extortion industry is, in Coveware's view, the best way to curtail its growth and corresponding impact to our Nation's public and private organizations.

The Economics of a Ransomware Attack

Following the three steps of a ransomware attack, we can illustrate the basic economics by breaking down the associated costs and expected proceeds.

1. **Gaining persistence:** The MOST common way that ransomware attacks occur is through compromised credentials to servers configured for remote access or Remote Desktop Protocol ("RDP"). There are groups, separate and apart from ransomware actors, that specialize in harvesting hundreds of thousands of stolen credentials from millions of exposed servers. The purchase of a set of credentials to a compromised RDP machine can be as inexpensive as $50 U.S. dollars.
2. **Detonation:** On a small network, there is little surveillance that needs to be done, so an actor may spend as little as a few hours on the network deploying the ransomware. For the sake of the exercise, let's assume this threat actor could earn $50 per hour elsewhere, and they spend 6 hours prepping the network for detonation. The total cost of

the actor's time is $300.

3. **Extortion:** The average ransom paid in Q2 of 2020 was $178,000 (See Appendix C).

Economic Arithmetic:

Total costs: $350
Total proceeds: $178,000
Total Profit: $177,650

Not all attacks are successfully monetized by the actor. Some companies are able to rebuild. Some companies are able to restore from backups. If we factor the total proceeds by a conversion rate of 25% (meaning they only get paid in 25% of the attacks they carry out, our economics are:

Total costs: $350
Total proceeds: $44,500
Total Profit: $44,150

The threat actors profit margin is over 99% (this is before cashout, which may reduce total proceeds through the laundering process). They probably invested a grand total of 12 hours in the attack across all phases. They have also taken virtually NO risk . All activity was conducted remotely over the internet and via proxies. The extortion negotiation was done over encrypted email or TOR chat service that is untraceable. The proceeds of the extortion are in cryptocurrency and may be moved anonymously through well established cash out channels.

The current profit margins of the cyber extortion industry is THE FUNDAMENTAL problem we need to address.

The cyber extortion industry is in a state of wild disequilibrium that favors the threat actors. Economics 101 predicts that this industry will continue to expand until the profitability decreases. This is why ransomware and cyber extortion attacks are proliferating.

The damage to the victim is not just the cost of the extortion though. Business interruption costs can be 5-100x larger than a ransom and can bankrupt a business as well. The cost of the interruption is where the economic pain inflicted on the U.S. economy is really felt. The median victim of a ransomware attack in Q2 of 2020 had less than 100 employees. Small businesses are the largest employer of our citizens and the backbone of the U.S. economy. For most of these companies, the question is when, not if, they will become a victim. Most do not believe they are targets.

Socio-Economic Enablers of Cyber Extortion Industry Growth

There are further socio-economic enablers that have propelled this industry into growth. In certain CIS and Eastern European states, there are large populations of STEM educated, working age individuals. They do not have legitimate employment prospects that can provide the financial earnings they desire. Accordingly, they participate in the cybercrime industry to pay their bills and feed their families. The jurisdictions where these populations live are generally beyond the reach of western law enforcement. Additionally, the capital that is returned to the local economies as a result of the cybercrime industry is substantial. These illicit proceeds support legitimate pillars of these local economies such as consumer goods spending and housing. The governments of these jurisdictions are therefore not particularly incentivized to curtail this criminal activity given the support it provides to the local economy. (source: "Industry of Anonymity: Inside the Business of Cybercrime," by Jonathan Lusthaus and "The Criminal Silicon Valley Is Thriving, New York Time Opinion by Jonathan Lusthaus 11/29/2019)

Technological Enablers of Cyber Extortion Industry Growth

As this industry has grown, it has also created innovations which allow for the participation of non-technical actors. One innovation of particular concern is known as Ransomware-as-a-Service (RaaS). As the name denotes, RaaS lowers the barrier to entry by automating many of the technical aspects of staging an attack. There are groups that provide RaaS kits, which are simple paint-by-numbers programs. These RaaS kits, along with written playbooks for non-technical actors, make staging an attack easy for non-technical individuals (see Appendix E). A new entrant to the cyber extortion industry can procure a RaaS kit for free, provided they split the extortion proceeds with the developer of the kit. The distributor then uses the RaaS kit in the same 3-step process described above, with similar economic outcomes. By enabling non-technical actors to become distributors of ransomware, the available population of willing participants is dramatically increased. This innovation has lowered a major barrier to entry. Whereas previously, an actor needed:

1. Technical capability necessary to carry out an attack
2. Financial motivation in excess of fear of criminal consequences
3. Access to the tools of the trade

Now actors no longer need technical skills, and access to tools has been made easy. The average dark marketplace has more available SKU's than a typical Home Depot (38,000+), the most commonly used of which are free.

~~1. Technical capability necessary to carry out an attack~~
2. Financial motivation in excess of fear of criminal consequences
~~3. Access to the tools of the trade~~

Consequently, the ONLY remaining barrier to entry is having enough financial motivation to overcome fear of the consequences. Violence in the cyber crime industry is extremely rare and almost a non-issue, especially as compared to other illicit industries such as narcotics or traditional organized crime. When set against the backdrop of a global pandemic and its economic consequences, it is clear why every day more and more people tip into participation in this industry.

This is a frightening picture of what awaits us if the unit-economics of cybercrime remain in disequilibrium. As long as the risk is low, the return is high and the addressable market of hungry participants is growing, this industry will continue to grow and the volume of attacks against organizations and enterprises in the U.S. will continue to rise.

The Role of the Private Cybersecurity Industry

Private security firms and services to enterprises can play an important role in applying pressure to the economics of the cyber extortion industry. Relative safety from these attacks is a function of resources, and there are too many organizations and enterprises that operate below the cyber security poverty line. This intangible line separates those that can afford to invest in best practices and technologies, and those that cannot or will not. Those that can afford to invest in security are still targets, but they are *too expensive of targets* to be considered by most financially motivated cyber criminals. Trying to break into a well fortified company for weeks on end is an economically irrational use of resources when there are plenty of cheaper targets. These targets are well below the cyber security poverty line and can be compromised with minimal time, effort, and cost.

Coveware believes that every private security company has an obligation to provide services that make it easier for organizations to lift themselves above the cyber security poverty line. The higher the threshold (i.e. cost) to pull off an attack, the lower the profitability for the cyber crime industry. While marketing buzzwords like ‘artificial intelligence’ and ‘machine learning,’ along with the latest zero-day exploit used by an APT get headlines, the reality is that the majority of the damage to our economy and public organizations is NOT caused by highly sophisticated APTs or nation-state actors. Damage to these organizations is caused by financially motivated cyber criminals using repetitive and unremarkable, but highly profitable, means of attack.

Recognizing the most common and economically favorable vectors of ingress, and helping organizations close the same, should be our top priority. The implementation of highly effective solutions does not need to be complex or costly, but is actually very straightforward and inexpensive. We think all software companies should take the fundamentals of our recommendations as a responsibility.

How to Reduce Exposure to Ransomware Attacks and Data Breaches

We suggest one simple initiative that will dramatically decrease the volume of attacks. This suggestion is rooted in our belief that in order to make substantive change, we must alter the economics of the cyber extortion industry. The industry’s profitability MUST be altered, otherwise it will continue to expand. While there are LOTS of ways to either increase costs, decrease revenue, or increase risk for cyber criminals, we must be pragmatic and work big-to-small. This does not mean other initiatives should be abandoned, it just means priority should be set based on the magnitude of the return on effort. We should do the things that have the greatest amount of impact using the least amount of resources in the shortest possible time.

Recommendation #1: Eliminate RDP as an attack vector

Since Coveware began collecting and reporting data (in Q3 of 2018), RDP has remained as the predominant attack vector. Compromised RDP credentials are used in 30-60% of ransomware attacks. This has not changed materially in 2 years. RDP is simply too cheap and reliable as a means to carry out an attack. Economically rational actors cannot ignore how profitable and predictable RDP based attacks are. There is no reason to use expensive 'zero-day' exploits or bespoke malware when less than $100 dollars allows a threat actor to gain access to a network. If compromised RDP credentials are eliminated or materially curtailed as an attack vector, the economic ripples to the cyber extortion industry will be material. First, the decrease in supply of credentials will lead to an increase in the price of whatever credentials remain available. A set of credentials that used to cost $50 may now cost $200. This will raise the barrier to entry as start up costs will increase, thereby decreasing the available labor pool of new criminals that can afford to participate. The decrease in supply of RDP credentials will put corresponding upward pressure on other means of attack, raising the cost as more actors that used to favor RDP are forced into higher cost activities. Since RDP attacks comprise roughly 50% of all attacks, the removal of these attacks would dramatically lower the average conversion rates, thereby lowering the expected proceeds of an attack. Additionally, swapping into alternative attack vectors would require more technical skills (along with capital). Removing non-technical actors from the available pool of participants would decrease the volume of attacks.

How do we close RDP as an attack vector for everyone?

The first step is recognizing how dangerous RDP is when misconfigured. A misconfigured RDP port is akin to globally advertising that you leave the front door of your home wide open. Threat actor specialists who run IP port scanning bots have emerged. These malicious programs scour every IP address on the internet, and can detect a new RDP port that is open misconfigured. A new RDP port will typically be discovered by one of these bots within 90 seconds of its first connection to the open internet (see Appendix F). The bot first locates the machine, and then immediately begins to brute force access. It will not stop until it is either locked out or has successfully guessed the user name and password.

Most organizations that misconfigure RDP do so out of convenience, with a misunderstanding of the risks. They assume they are too small to be a target, and don't bother to take the proper precautions. As we have described above, anyone that opens RDP to the internet is a target. There are currently close to 4.7 million misconfigured RDP machines open to the internet. The supply is massive, making the corresponding cost of compromise low. Until this is fixed, the attacks will continue.

Properly Configuring RDP

We have provided a simple guide in Appendix G that outlines the proper steps to configure RDP. What is important to recognize is that applying proper RDP configuration DOES NOT require the purchase of expensive hardware or software. It only requires the awareness of this risk, and the time and effort to patch the issue. We offer it as the main recommendation of this testimony BECAUSE of its simplicity AND the relatively high impact it could have given the minimal investment necessary. The Committee has specifically requested what steps "resource-constrained enterprises and organizations (both public and private) can take to reduce their exposure." Coveware can offer no greater recommendation that has so substantial a return on investment given how common RDP based ransomware attacks are. The fix only requires awareness and time and effort to properly configure. The result could lead to a dramatic reduction in attacks, and corresponding decrease in the profitability of the cyber extortion industry. If we are able to eliminate or significantly curtail RDP as an attack vector, we will tip the industry's unit economics away from the criminals.

RDP Case Study - Proof this will work

In April of 2020 a well known cyber insurance company launched an initiative to reduce the number of RDP based ransomware attacks claimed by their policyholders. In order to do so they proactively scanned their policy holders for vulnerability, screened renewals and new applications for exposed RDP, and then provided remediation steps to the policy holders. They followed up with all their policyholders and even offered financial incentives, via lower policy premiums, to organizations that took their mitigation steps. In the 4 months that followed the launch of this initiative, their total volume of ransomware claims dropped by 65%. RDP was virtually eliminated as an attack vector for the claims they did receive. There is nothing special about this single insurance company's policy holders, they are the same size and shape our Nation's small businesses and public sector organizations. The same results are possible across a broader swath of exposed organizations.

Recommendation #2: Require multi-factor authentication for Administrative Users.

While we would prefer ALL users of a network be required to pass through multi-factor authentication, we are pragmatists and recognize that a lot of organizations simply won't deploy these requirements to their users. Our recommendation is that administrative systems like Active Directory, security applications, and back up systems require an administrator to authenticate with two factors. In the history of Coveware, spanning thousands of attacks on companies large and small, we have NEVER seen multi-factor authentication overcome by a threat actor.

Conclusions

Threats to enterprises and organizations from the cyber extortion industry will never disappear, but the depth and impact of this criminal industry on our country is fully within our control. Applying an economic lens to the problem, and working big-to-small as we have suggested, will tip the industry into contraction. We will never be free of threats, but we must turn the tides of this criminal industry and minimize the impact it has on our country. When combined with new security policy and a healthy dose of law enforcement, we see a very different future that is both practical and achievable. It would not take years to correct, and most importantly, it does not require a massive increase in spending. All it takes is awareness, understanding, and willpower.

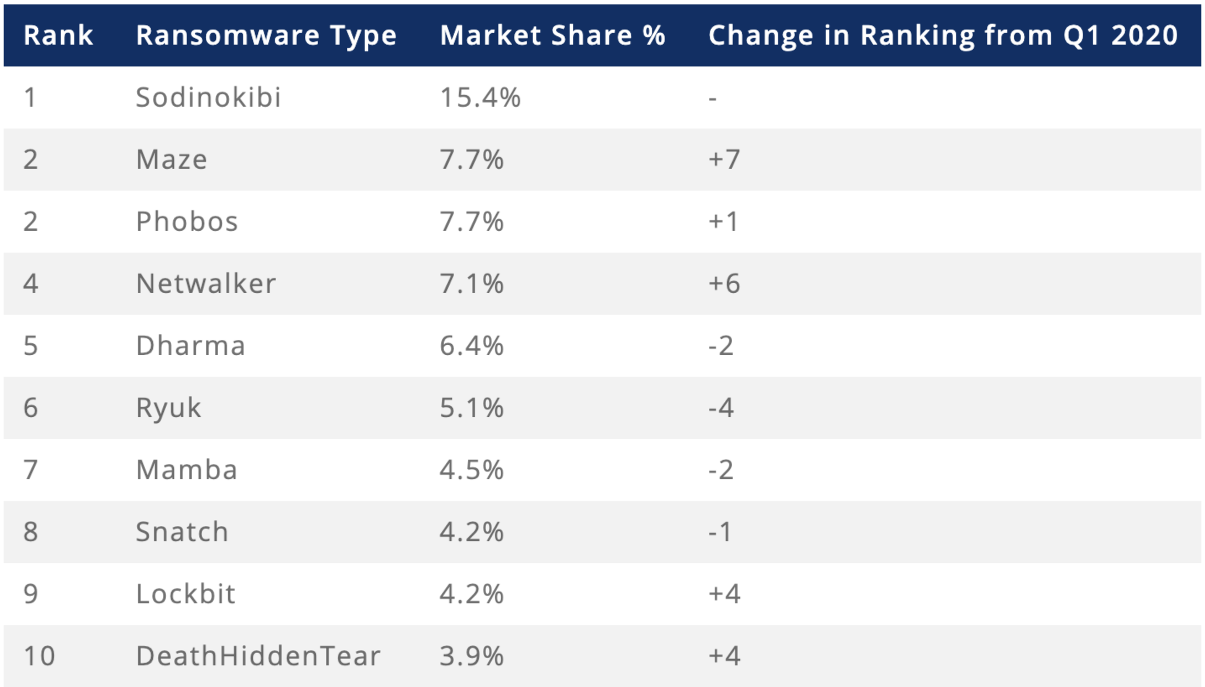
Thank you for your time.

~Bill Siegel
CEO and Co-Founder of Coveware

Appendices

Appendix A

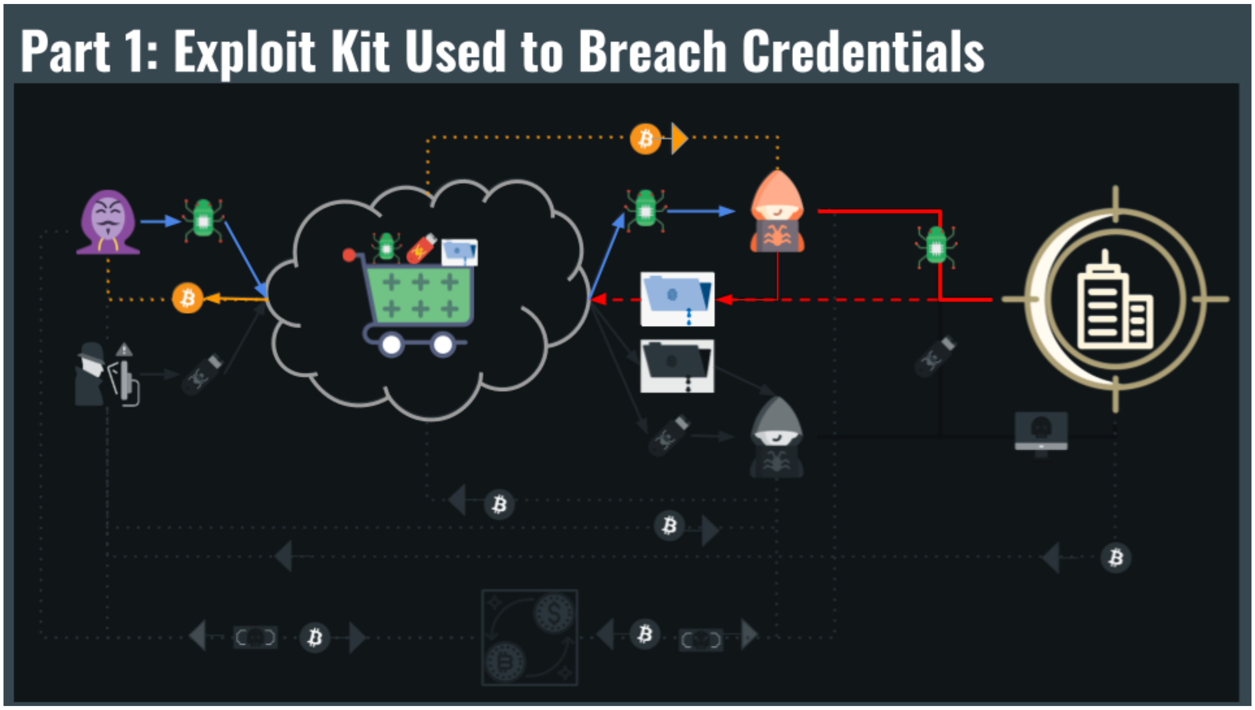
Common Ransomware groups by market share of attacks

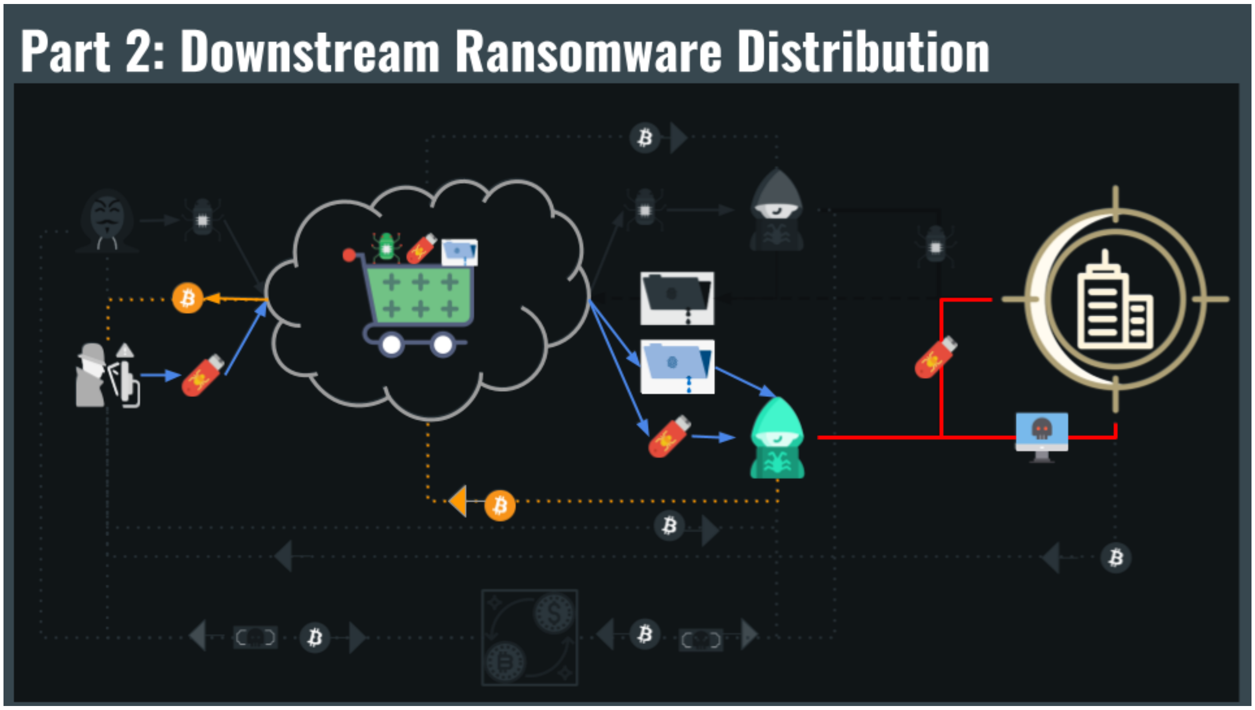


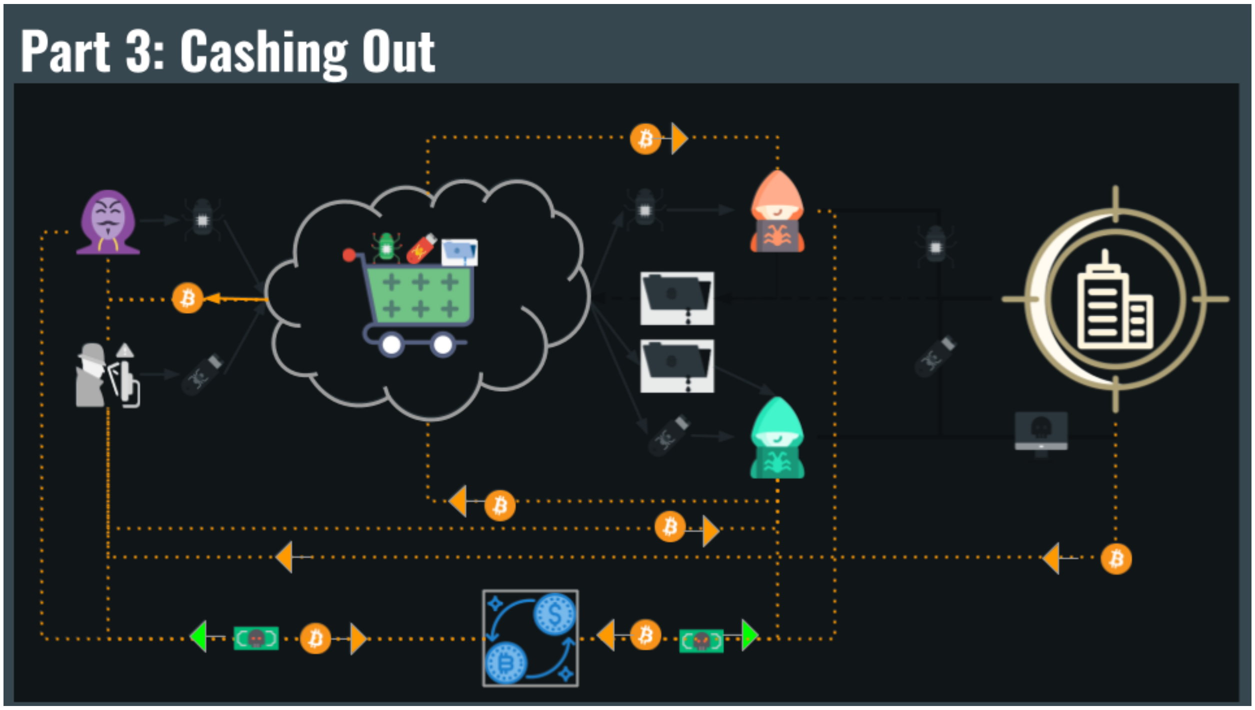
Rank	Ransomware Type	Market Share %	Change in Ranking from Q1 2020
1	Sodinokibi	15.4%	-
2	Maze	7.7%	+7
2	Phobos	7.7%	+1
4	Netwalker	7.1%	+6
5	Dharma	6.4%	-2
6	Ryuk	5.1%	-4
7	Mamba	4.5%	-2
8	Snatch	4.2%	-1
9	Lockbit	4.2%	+4
10	DeathHiddenTear	3.9%	+4

Appendix B

Flow chart of a typical ransomware attack showing different industry groups, specialists, and coordination.



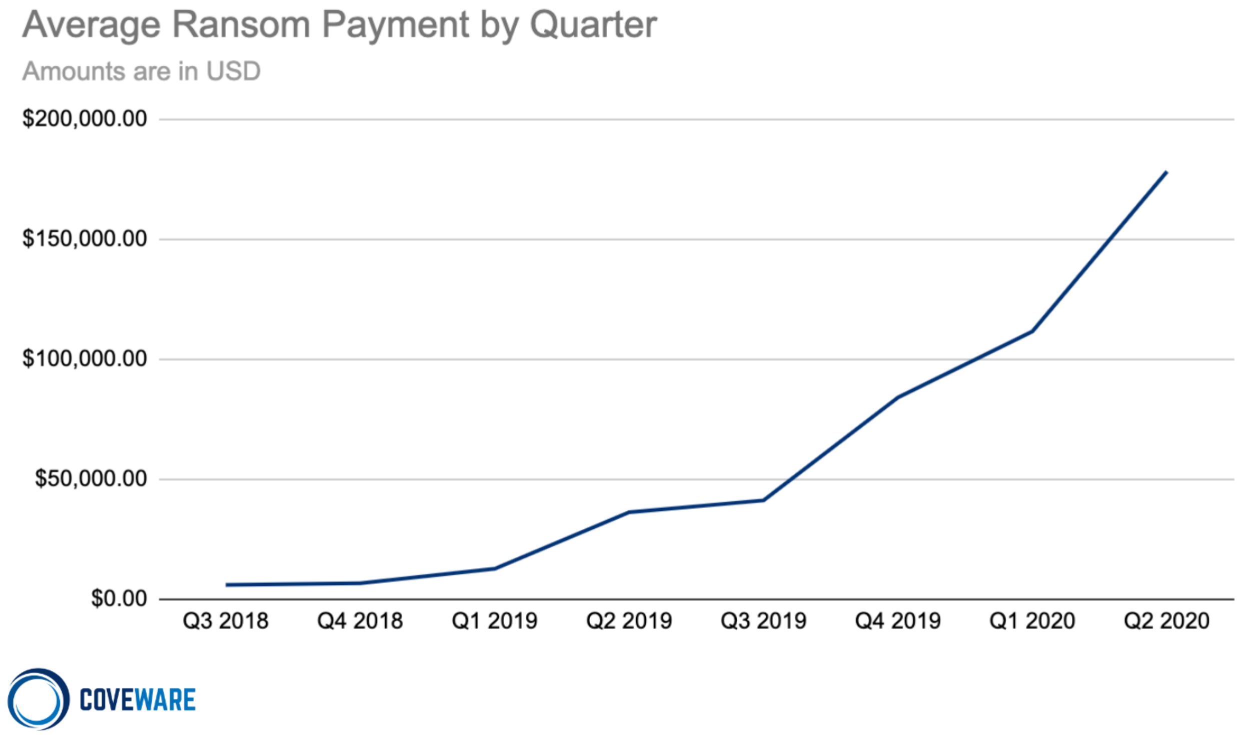




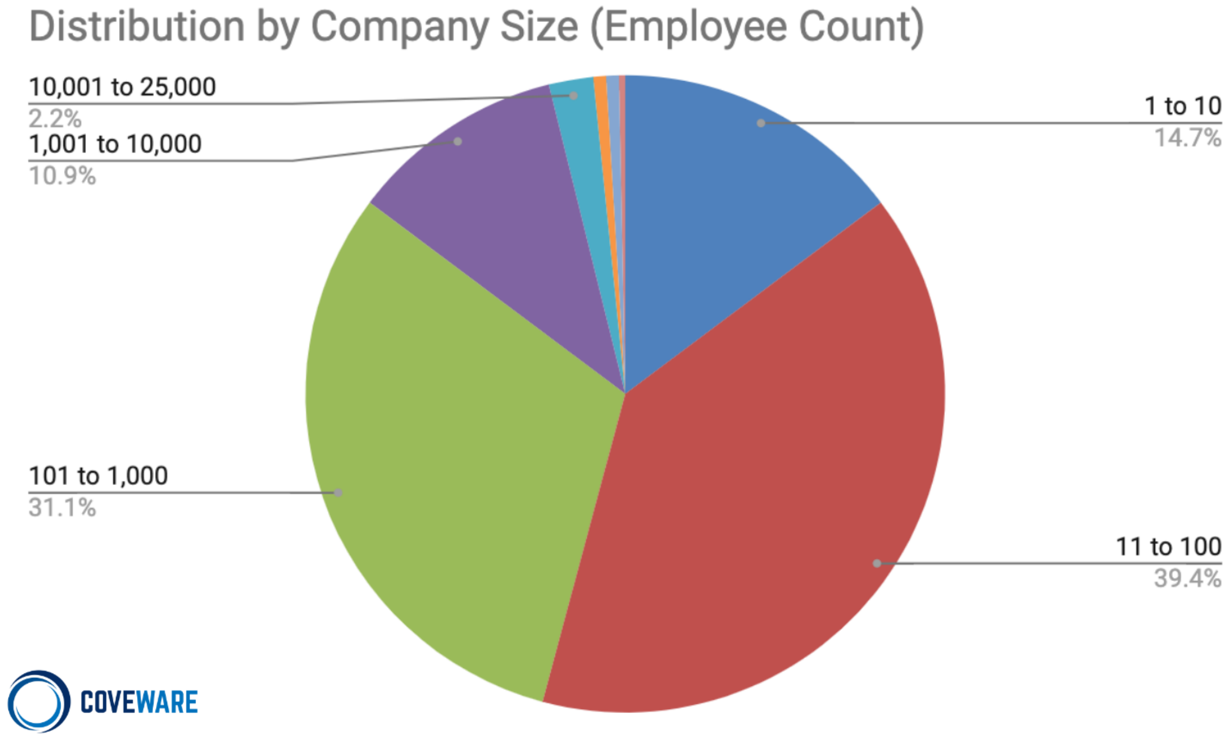
Part 3: Cashing Out

Appendix C

Increasing size of average ransom payments

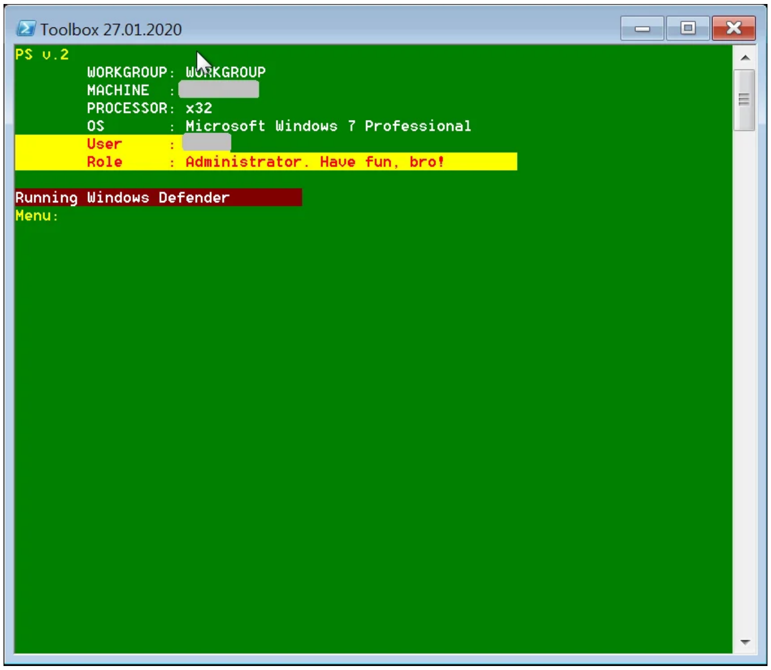


Appendix D:
Average size of a company impacted by ransomware in Q2 2020.

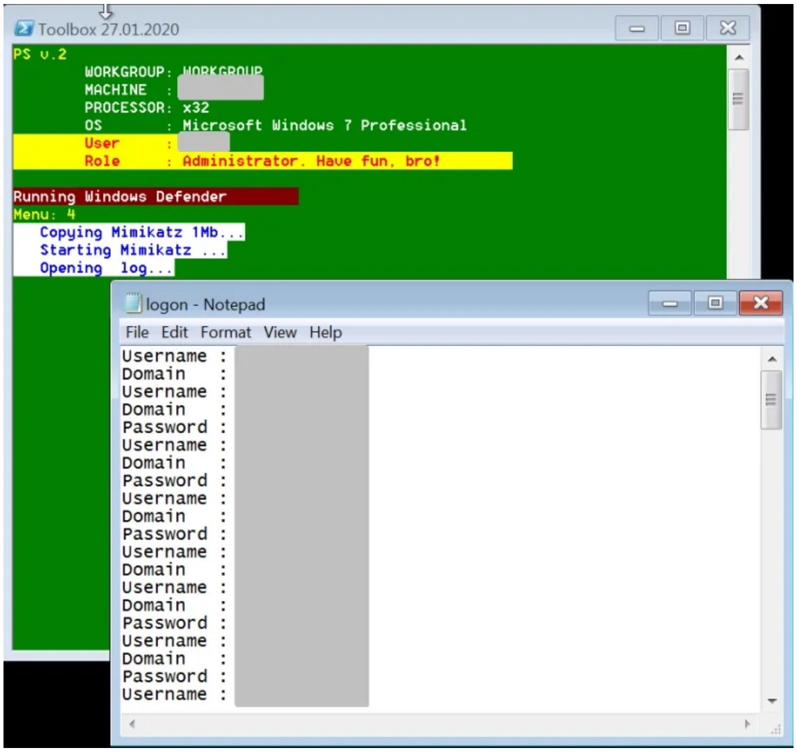


Appendix E:

Examples of simple to use, Ransomware-as-a-Service kits



```
PS v.2
        WORKGROUP: WORKGROUP
        MACHINE  : [redacted]
        PROCESSOR: x32
        OS       : Microsoft Windows 7 Professional
        User     : [redacted]
        Role     : Administrator. Have fun, bro!

Running Windows Defender
Menu:
```



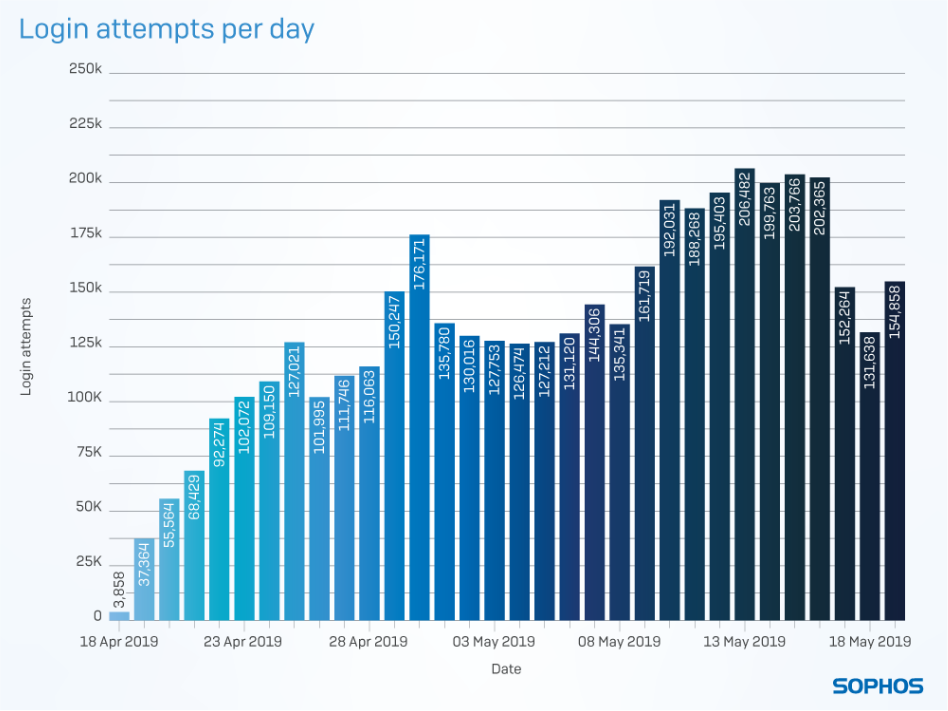
```
PS v.2
        WORKGROUP: WORKGROUP
        MACHINE  : [redacted]
        PROCESSOR: x32
        OS       : Microsoft Windows 7 Professional
        User     : [redacted]
        Role     : Administrator. Have fun, bro!

Running Windows Defender
Menu: 4
   Copying Mimikatz 1Mb...
   Starting Mimikatz ...
   Opening  log...
```

```
Username : [redacted]
Domain   :
Username :
Domain   :
Password :
Username :
Domain   :
Password :
Username :
Domain   :
Password :
Username :
Domain   :
Username :
Domain   :
Password :
Username :
Domain   :
Password :
Username :
```

(Source: Sophos & BleepingComputer)

Appendix F:

Login attempts over a 30 day period on a standard, improperly secured RDP machine



(Source: Sophos)

Appendix G:

Common steps to properly secure RDP:

1. Proactively apply OS and software patches: Keep OS and RDP related software up to date. Don’t wait for something to break.
2. Strong Passwords and MFA: RDP connections should require strong passwords and multi-factor authentication (either at VPN or RDP level).
3. Limit Access or White List IP Address: Access granted only via a VPN session or only to a select whitelist of IP ranges.
4. Lockout: Access should be blocked after a short number of login attempts fail to prevent brute forcing.
5. The default port number should be changed from default (3389) to a random port number.
6. No exceptions. If a manager or noisy user constantly complains about tedious RDP security protocols then their RDP privileges should be put on warning.