A Tale of Epic Extortions

How Cybercriminals Monetize Our Online Exposure

Authors: Digital Shadows Photon Research Team

digital shadows_

Executive Summary

- **With unwanted online exposure, it's not just account takeover and fraud you need to worry about. Cybercriminals can also monetize your exposure through extortion-based attacks.** They're taking advantage of compromised credentials; sensitive data, such as documents or intellectual property; and technical vulnerabilities on Internet-facing applications.

- **Using compromised credentials found on public websites, spammers amassed over $330,000 through sextortion campaigns in 2018.** Across a sample of 792,000 emails tracked by Digital Shadows, extortionists used exposed credentials found on public lists and paste sites to convince victims they had been compromised.

- **Crowdfunding models allow extortionists to raise funds from the general public, rather than rely on victims giving in to ransom demands.** Anyone dealing with sensitive, inflammatory or sensational information should ask themselves: How would we respond if an attacker chose crowdfunding over direct extortion?

- **Vulnerabilities on Internet-facing applications can be monetized and exploited by attackers looking to deploy ransomware.** Attackers such as the SamSam group combine active and passive scanning to find exploitable targets, which can end in significant disruption and financial loss, draining your capacity to conduct normal business.

- **The barriers to entry for extortion-based activity continue to fall. Extortionists come in all shapes and sizes, with varying levels of sophistication.** With account, database and network accesses available on criminal forums, and extortion guides for sale at under $10, aspiring extortionists have a wealth of resources to get started.

- **More experienced extortionists are promising salaries of over $30,000 through tutorials and recruitment opportunities.** Posts on message boards and forums claim new recruits can make a decent living through cyber sextortion scams directed at high-worth individuals like executives, lawyers, and doctors.

- **There are ways to take back control and reduce extortion risks if businesses and individuals properly manage their digital footprints and online exposure.** You can drastically lower your chances of falling victim to extortion by: creating a response playbook—such as for ransomware scenarios, improving your data loss detection, practicing good credential hygiene, and reducing your attack surface.

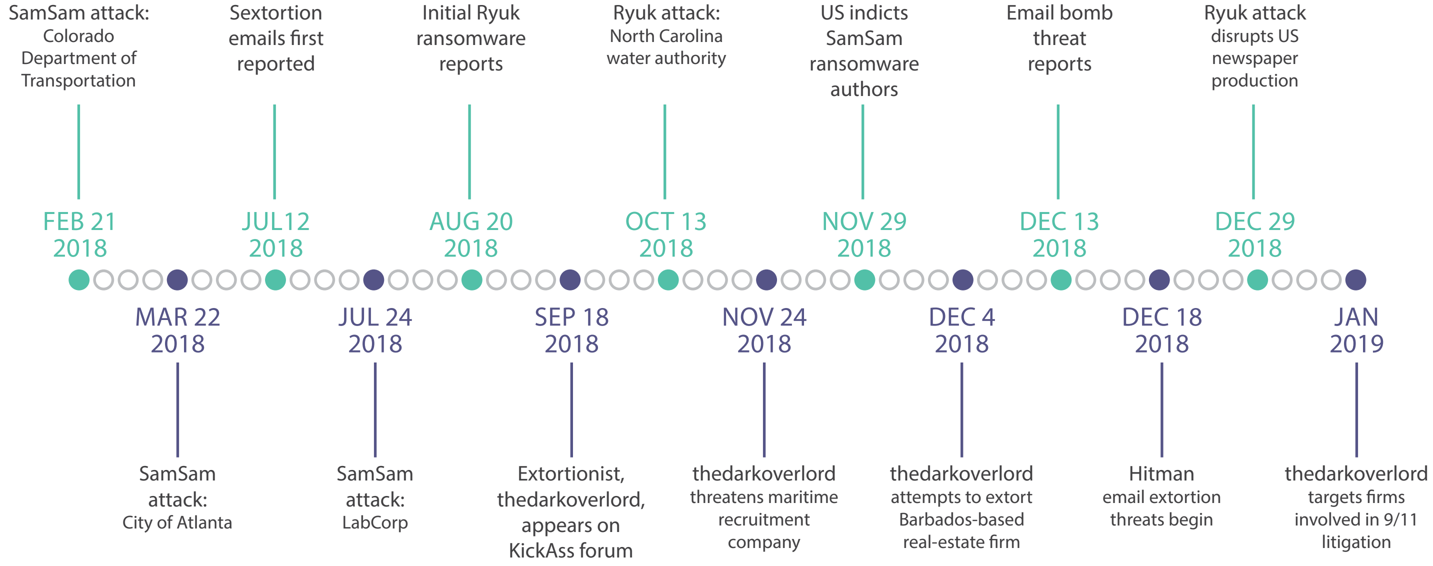
Table of Contents

1. A Tale of Epic Extortions:
Introduction

Not long ago, online extortion typically involved blackmailers sending threatening emails to their victims, promising to leak compromising information. Other extortionists tried warning victims of an impending cyber attack, such as a denial of service (DoS) attempt if ransom demands were not met. In the early 2010s, ransomware emerged as a viable method of coercion, culminating in the 2017 "WannaCry" attack that crippled business operations in over 100 countries.

Although these techniques are still popular, Digital Shadows has found that cybercriminals have diversified their extortion methods. Looking at some of the most significant extortion-based activity over 2018, we can see that the threat landscape is as wide and varied as it's ever been (see Figure 1).

Figure 1: Timeline of selected extortion attacks in 2018 and 2019



FEB 21 2018
SamSam attack: Colorado Department of Transportation
MAR 22 2018
SamSam attack: City of Atlanta
JUL12 2018
Sextortion emails first reported
JUL 24 2018
SamSam attack: LabCorp
AUG 20 2018
Initial Ryuk ransomware reports
SEP 18 2018
Extortionist, thedarkoverlord, appears on KickAss forum
OCT 13 2018
Ryuk attack: North Carolina water authority
NOV 24 2018
thedarkoverlord threatens maritime recruitment company
NOV 29 2018
US indicts SamSam ransomware authors
DEC 4 2018
thedarkoverlord attempts to extort Barbados-based real-estate firm
DEC 13 2018
Email bomb threat reports
DEC 18 2018
Hitman email extortion threats begin
DEC 29 2018
Ryuk attack disrupts US newspaper production
JAN 2019
thedarkoverlord targets firms involved in 9/11 litigation

In the past year extortion emails have threatened physical harm and the release of sexually explicit content. Some cybercriminals have experimented with crowdfunding platforms as an alternative way to collect their extortion demands. With ransomware, we saw the SamSam group's variant eschew traditional phishing and exploit kit delivery methods. Instead it exploited vulnerabilities in public-facing servers and harvested administrator credentials to self-propagate and disrupt entire networks, meaning its operators could demand significantly higher ransoms.

SamSam
Ransomware variant active since 2015; exploits JBoss software. Used in attacks against organizations in the US, Europe and Asia.

Sextortion
Spam campaign claiming to have footage of recipient watching pornography. Included threats to publicly release video.

Hitman
Spam campaign claiming recipient was to be killed unless Bitcoin demand was paid.

thedarkoverlord
Extortionists known for high-profile campaigns against healthcare and entertainment industries.

Ryuk
Ransomware variant active since 2018. Evolved from the "Hermes" variant, and delivered via phishing or "Emotet" and "Trickbot" campaigns.

How Cybercriminals Monetize Our Online Exposure

When it comes to extortion, threat actors need something valuable to be able to perform their attack and strong-arm victims into paying up. This could be details of someone's private life, confidential company information, or, in the case of SamSam, complete control over an organization's network.

Acquiring this information or privileged access has never been easier. As businesses rush into digital transformation, and new individuals and services join the digital economy daily, it's becoming harder and harder to manage our data and digital assets. Cybercriminals recognize this and have developed ways to profit from our unwanted online exposure through extortion-based attacks. In the subsequent sections, we outline three main types of exposure extortionists are taking advantage of:

1. Compromised credentials

Attackers use cheap and readily available breached credentials to perform mass extortion campaigns and convince victims they have been breached.

2. Sensitive data

Not only will they extort you directly, cybercriminals have dedicated sections on online forums to sell sensitive data, such as corporate documents and intellectual property. Crowdfunding models also offer them an alternative way to raise revenue from the general public instead of relying on victims to pay ransom demands.

3. Technical vulnerabilities

Attackers can perform active and passive scanning to identify exploitable vulnerabilities on Internet-facing applications. They can then deploy ransomware variants that not only disrupt your business and damage its reputation, but also demand sizeable ransom fees to cease attacks.

2. Sextortion Diaries:
Monetizing Compromised Credentials

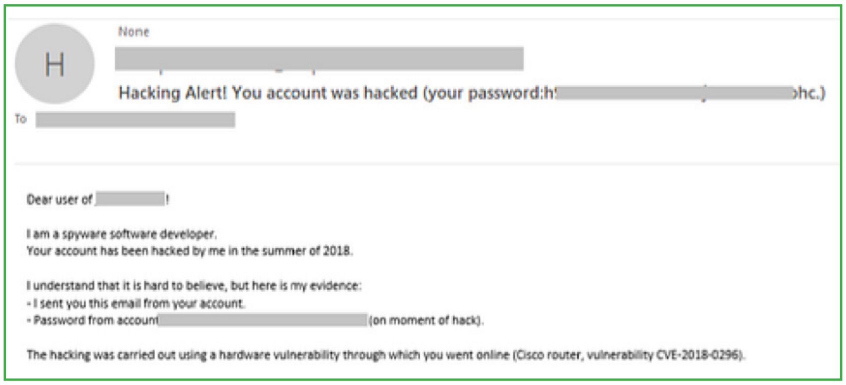
When we think of potential uses for breached or compromised username-password combinations, we tend to think of a criminal taking over our email accounts or trading our credentials on criminal forums and marketplaces. When such credential sets are no longer valid, their value becomes almost negligible; that's why large breached data sets that have been around for years are freely shared and re-posted online. Extortionists, however, have developed new ways to profit from these easily available credential sets.

Sextortion-based email campaigns seek to extort victims by threatening to publicly embarrass them for engaging in a sexually explicit act. They claim to have evidence and use previously exposed passwords as "proof" of compromise. These emails have been reported intermittently since late 2017, but the scale and persistence of the campaigns rocketed over 2018. Between July 2018 and February 2019, Digital Shadows has collected and analyzed a sample of sextortion emails in which 89,000 addresses received over 790,000 sextortion attempts.

Uncovering sextortion: July 2018 - February 2019

89k	792k	3,100+	92	$332k
Email recipients	Total attempts against target emails	Unique sender Bitcoin addresses	Bitcoin addresses that received payments	Value of total extortion payments received

The emails have followed a similar pattern: The extortionist provides the user with a known password as "proof" of compromise, then claims to have video footage of the victim watching adult content online, and finally urges them to pay a ransom to a specified Bitcoin (BTC) address. A later iteration of the campaign involves the extortionist trying to support their credibility by sending another email that refers to a Cisco ASA router vulnerability (CVE-2018-0296) . The extortionist suggests that the vulnerability allowed them to access the victim's machine (see Figure 2 below).



H

None

[redacted]

Hacking Alert! You account was hacked (your password:[redacted])

To [redacted]

Dear user of [redacted]!

I am a spyware software developer.
Your account has been hacked by me in the summer of 2018.

I understand that it is hard to believe, but here is my evidence:
- I sent you this email from your account.
- Password from account[redacted](on moment of hack).

The hacking was carried out using a hardware vulnerability through which you went online (Cisco router, vulnerability CVE-2018-0296).

Figure 2: Example of sextortion email referring to compromised credentials and Cisco vulnerability

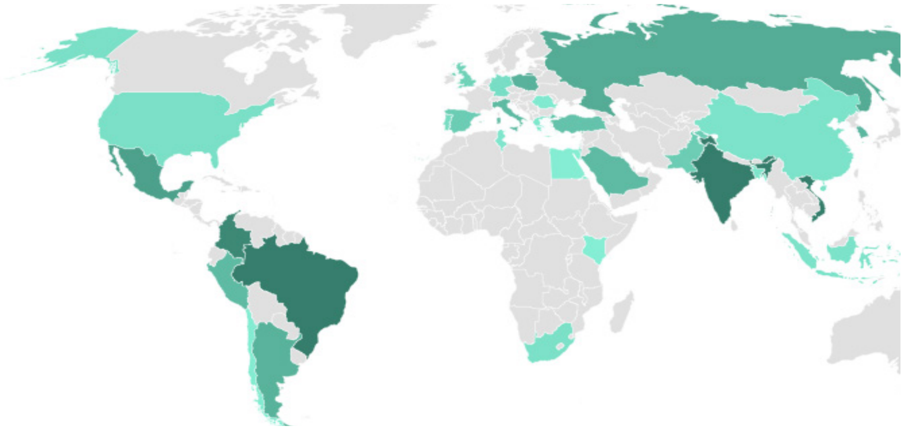
2. Sextortion Diaries:
Monetizing Compromised Credentials

Across the emails we collected, there was a variation in the capabilities displayed by the attackers. Certain spammers showed little understanding of how to craft and distribute emails on scale, sending malformed emails that would never make it past a mail server or spam filter.

Conversely, some of the campaigns were clearly well-coordinated, with emails sent from newly created outlook.com email addresses. In some instances, the local-part of the sender's email address (local-part@domain.com) was randomly generated. As these emails don't appear in previous public breaches, attackers may have created specific addresses for these campaigns rather than relying on using compromised accounts for email distribution.

These campaigns are also truly global operations, with servers based across at least five continents. According to sender IP location information, the highest proportion of emails in our sample were sent from Vietnam (8.5%), followed by Brazil (5.3%) and India (4.7%). While this can give us some indication of where the attackers are based, many of these could also be cases where email servers have been compromised and used for spam campaigns.

Figure 3: Sextortion email sender's IP address location by country



In the bluff: New uses for compromised credentials

Although our sample set represents only a small proportion of these sextortion emails, it highlights how attackers are finding financial gain through breached credentials in innovative ways. Across our sample, the most popular breaches were the Anti Public Combo and the Exploit IN leaks: 66 percent of the credentials listed in the sample matched the Anti Public Combo list, while 58 percent were present in the Exploit.in breach. (The total exceeds 100 percent as some credential sets appeared in multiple breaches.)

Of course, an attacker with genuine access to a victim's machine would have a host of other options available to profit from. This could include logging into online banking sessions, harvesting personally identifiable information (PII) to sell or use for fraud, or stealing sensitive documents. Email access would also provide a perfect platform for a business email compromise campaign, where cybercriminals will take over an email account and use it to make wire fund requests from employees and suppliers.

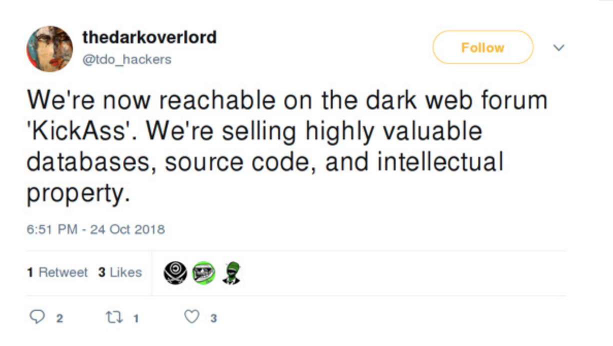
3. Ransom by Popular Demand: *Monetizing Sensitive Data*

During the second half of 2018, extortionist thedarkoverlord (TDO) reemerged from a brief hiatus, this time with a different style of play. Rather than extort victims directly, TDO looked to sell stolen data in batches to other users on criminal forums, and adopted an altogether more unusual tactic: online crowdfunding campaigns.

Thedarkoverlord Sales:

Peddling ready-made extortion data

When TDO first appeared, the threat actor used TheRealDeal, a dark Web (criminal) forum to sell data sets they had allegedly obtained by breaching victim organizations. After TheRealDeal folded , TDO began a wave of extortions that involved contacting victims directly and demanding ransom payments to prevent the public release of sensitive information, such as health records and medical scans. Simultaneously, TDO publicized this activity via Twitter, taunting victims (see Figure x).

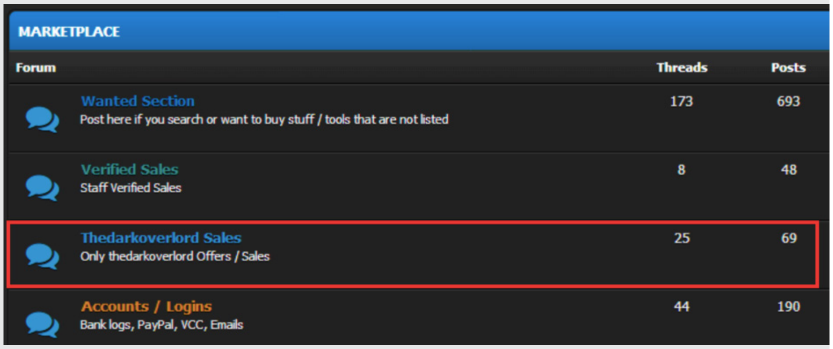


We're now reachable on the dark web forum 'KickAss'. We're selling highly valuable databases, source code, and intellectual property.

6:51 PM - 24 Oct 2018

1 Retweet 3 Likes

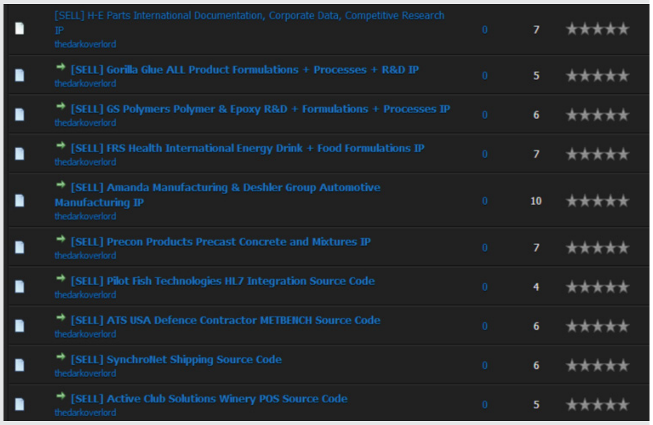
Figure 4: TDO advertising their presence on KickAss forum via Twitter



MARKETPLACE

Forum	Threads	Posts
Wanted Section Post here if you search or want to buy stuff / tools that are not listed	173	693
Verified Sales Staff Verified Sales	8	48
Thedarkoverlord Sales Only thedarkoverlord Offers / Sales	25	69
Accounts / Logins Bank logs, PayPal, VCC, Emails	44	190

Figure 5: Thedarkoverlord Sales subsection of KickAss



[SELL] H-E Parts International Documentation, Corporate Data, Competitive Research IP thedarkoverlord	0	7	★★★★★
[SELL] Gorilla Glue ALL Product Formulations + Processes + R&D IP thedarkoverlord	0	5	★★★★★
[SELL] GS Polymers Polymer & Epoxy R&D + Formulations + Processes IP thedarkoverlord	0	6	★★★★★
[SELL] FRS Health International Energy Drink + Food Formulations IP thedarkoverlord	0	7	★★★★★
[SELL] Amanda Manufacturing & Deshler Group Automotive Manufacturing IP thedarkoverlord	0	10	★★★★★
[SELL] Precon Products Precast Concrete and Mixtures IP thedarkoverlord	0	7	★★★★★
[SELL] Pilot Fish Technologies HL7 Integration Source Code thedarkoverlord	0	4	★★★★★
[SELL] ATS USA Defence Contractor METBENCH Source Code thedarkoverlord	0	6	★★★★★
[SELL] SynchroNet Shipping Source Code thedarkoverlord	0	6	★★★★★
[SELL] Active Club Solutions Winery POS Source Code thedarkoverlord	0	5	★★★★★

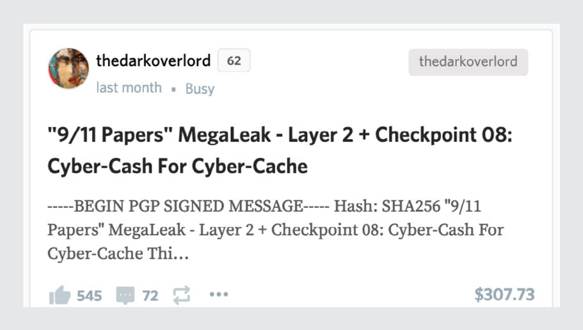
Figure 6: Corporate data, intellectual property and source code advertised via Thedarkoverlord Sales

Around September 2018, TDO reestablished a presence on the criminal forum scene, appearing on the hacking and insider community known as KickAss (Figure 4). As well as using KickAss to recruit accomplices for their extortion enterprise, TDO once again used the forum as a platform to profit from acquired data sets. They set up a dedicated subsection of KickAss, known as Thedarkoverlord Sales, to sell stolen data to other extortionists and fraudsters (Figures 5 and 6 left).

3. Ransom by Popular Demand: *Monetizing Sensitive Data*

From KickAss to KickStarter: 9/11 papers and the crowdfunding model

In April 2018 TDO stole documents belonging to the insurance provider Hiscox. These included files related to the September 11, 2001 (9/11) terrorist attacks in the US, mainly comprised of litigation papers and insurance claims for victims. TDO released what they said was the entire trove of data (about 10GB worth) as an encrypted cache of files with five main sections, each with its own decryption key. TDO began crowdfunding the publication of these keys if certain milestones (Bitcoin payment amounts) were hit, intending to pressure Hiscox and the other companies mentioned in the stolen documents to pay up (Figure 7). The insinuation by TDO was that the papers would paint the insurers and their clients in a bad light for the way they handled 9/11 compensation claims.



"9/11 Papers" MegaLeak - Layer 2 + Checkpoint 08: Cyber-Cash For Cyber-Cache

-----BEGIN PGP SIGNED MESSAGE----- Hash: SHA256 "9/11 Papers" MegaLeak - Layer 2 + Checkpoint 08: Cyber-Cash For Cyber-Cache Thi...

Figure 7: TDO crowdfunding post related to 9/11 papers

With the success of legitimate crowdfunding platforms, such as Patreon and KickStarter, TDO has adopted the same kind of model for extortion data leaks. This is a great example of how cybercriminals continue to borrow legitimate commercial business models in their criminal pursuits. In true TDO style, the use of a crowdfunding platform has allowed them to increase their publicity in the online community, while providing an additional revenue stream for their extortion antics.

When Plan A fails

When victims refuse to meet ransom demands, extortionists are usually forced to deliver on their threats and leak the data publicly, receiving no financial reward for their efforts. With Thedarkoverlord Sales subsection of KickAss, and the crowdfunding model, we see how TDO has resorted to alternative ways to make money off stolen data they might otherwise have had to publish. Rather than rely on victims, TDO hopes to play on the public's appetite for 9/11-related controversy, and encourage them to raise the funds. Maybe this is an indication that victims are no longer giving in to TDO's demands. Or it could signal a new method of extortion future cybercriminals will seize upon.

This type of extortion routine is not new. In 2016 we wrote about the potential for crowdsourced extortion attempts to become more popular following a spate of Mirai botnet DoS attacks. A similar kind of extortion routine was orchestrated by the "Shadow Brokers" after that threat group leaked alleged US National Security Agency (NSA) tools, including the ETERNALBLUE exploit used in the WannaCry and "NotPetya" cyber attacks in 2017.

With approximately $11,600 (BTC 3.46) currently accumulated in the Bitcoin wallet TDO used for the 9/11 leaks, the jury is still out on the crowdfunding model. We can expect to see more cybercriminals try their luck with this extortion tactic. In particular, they might favor crowdfunding if they have sensitive information they believe will garner widespread public interest (think Panama Papers). Organizations dealing with such inflammatory or sensational information should consider how they would respond if an attacker takes this course of action.

*The price of Bitcoin is extremely volatile. This pricing was assessed in February of 2019.

4. SamSam but Different: *Monetizing Technical Vulnerabilities*

On November 28, 2018 the US Department of Justice (DoJ) unsealed an indictment against two Iranian nationals. Known collectively as the SamSam group, they deployed ransomware to extort hospitals, municipalities, and public institutions, causing over $30 million in losses. The attackers targeted a wide range of organizations, including:

- Multiple healthcare service providers
- City of Atlanta
- City of Newark
- Colorado Department of Transportation
- Hollywood medical center
- Kansas Heart Hospital
- Port of San Diego
- University of Calgary

Judging by the opportunistic style of the attacks, it seems these organizations were targeted because the attackers believed they could compromise their networks and successfully deploy ransomware, as opposed to targeting them specifically for the nature of their work.

Extorting known security vulnerabilities

Unlike other actors performing targeted attacks, the SamSam group did not rely heavily on spearphishing for their initial access method. According to the indictment, the attackers used two main methods to gain initial access:

1. Exploiting public-facing applications
2. Abusing valid accounts for remote-access systems

The SamSam group exploited vulnerabilities in JBoss servers , FTP servers and, potentially, Server Message Block (SMB) servers . They relied on organizations not patching their software against known vulnerabilities with publicly available exploits. The group then used their initial access to extort the organization. This is a clear example of how attackers can profit from an organization's security vulnerabilities: through the medium of extortion.

The attackers also abused valid credentials for remote-access solutions, namely through a remote desktop protocol (RDP) brute-force cracking tool. "NLBrute" allows an attacker to try combinations from a wordlist (a collection of known or often-used usernames and passwords) against multiple target RDP servers, to see which sets of credentials are valid.

Despite repeated warnings on how threat actors identify and exploit public-facing services , we're still providing ample opportunities for cybercriminals like the SamSam group to prosper. At the time of writing, there were over 3.6 million RDP servers available on the public Internet, and upwards of 34,000 JBoss servers.

Given these approaches, it's likely the SamSam group performed a combination of active and passive scanning to identify exploitable targets. The attackers also may have used breached data and brute-force cracked or stolen credentials to gain initial access to the target environments.

With the exploitation of known, public vulnerabilities and poorly configured authentication systems, we see how the risks of security debt (the accumulation of unpatched systems, exposed services, etc.) extend beyond the theoretical. The SamSam group's attacks led to financial losses for organizations, and significant disruption that hindered the ability to conduct normal business.

MITRE ATT&CK and the SamSam Group

The Photon Research Team have used the MITRE ATT&CK™ framework to map the tactics, techniques, and procedures detailed in the indictment and provide key lessons for organizations to take away. Additional on the tooling used for the SamSam ransomware attacks are available in the Avoiding the Shakedown section of this report.

Mitre ATT&CK Stage	SamSam TTPs	Mitigation Advice
0. Reconnaissance	Technical information gathering; Technical weakness identification	• Carefully consider which services should be Internet facing, to reduce the risk of opportunistic exploitation • Create an inventory of software and services connected to the public-facing Internet, to prioritize patching
1. Initial Access	Exploitation of public-facing application; valid accounts	• As a priority, patch any in-the-wild exploit for software or a service in the inventory • Ideally, make remote-access solutions (such as RDP) accessible only over a virtual private network (VPN); where not possible, use access control lists to restrict which IP address ranges can connect to the service • At a bare minimum, configure lock-out policies to mitigate brute-force cracking attacks
2. Execution	Command line; GUI; Windows Management Instrumentation (WMI)	• Monitor execution of WMI, PowerShell, and other system administration tools for visibility into potential attacker activity (e.g. execution of WMI commands by non-admin users who have never executed WMI before)
3. Persistence	External remote services; path interception	• If an account is suspected to be compromised, revoke credentials so that the attackers cannot trivially regain access to the target environment • Eliminate unquoted service paths • Log command line activity for tracking script execution
4. Privilege escalation	Dynamic Link Library (DLL) search order hijacking	• Run public tool sets in controlled environment • Ensure that there are no unquoted service paths in the default set of environment variables and that all DLLs expected to be loaded exist on the file system

MITRE ATT&CK and the SamSam Group

Mitre ATT&CK Stage	SamSam TTPs	Mitigation Advice
5. Defense Evasion	Disabling security tools	• Consider any disablement of an Endpoint Protection Platform (EPP) product a red flag visible in the operating system (OS) logs or in a SIEM product
6. Credential Access	Credential dumping	• Control access to administrator privileges as a top priority to mitigate credential dumping attacks • Practice robust logging and alerting to complement an Endpoint Detection and Response (EDR) system by providing detailed information on OS activity that could indicate the use of tools like Mimikatz, such as via wmiexec
7. Discovery	Remote system discovery; system information discovery	• Use monitoring to raise alerts of internal port scans or bulk Lightweight Directory Access Protocol (LDAP) queries • Ensure vulnerability (VA) scans are appropriately whitelisted • Use application whitelisting features, such as Microsoft AppLocker, to detect (and potentially block) application executions • Trace which LOLBAS (Living Off the Land Binaries And Scripts) are executing
8. Lateral Movement	Service execution	• Restrict workstation-to-workstation communication (via firewalling or even private Virtual Local Area Networks [VLANs]) • Apply principle of least privilege to ensure only necessary personnel have the administration privileges required for certain actions
9. Command and Control	Remote-access tools	• Regularly review remote-access logs to ensure no unauthorized access has taken place

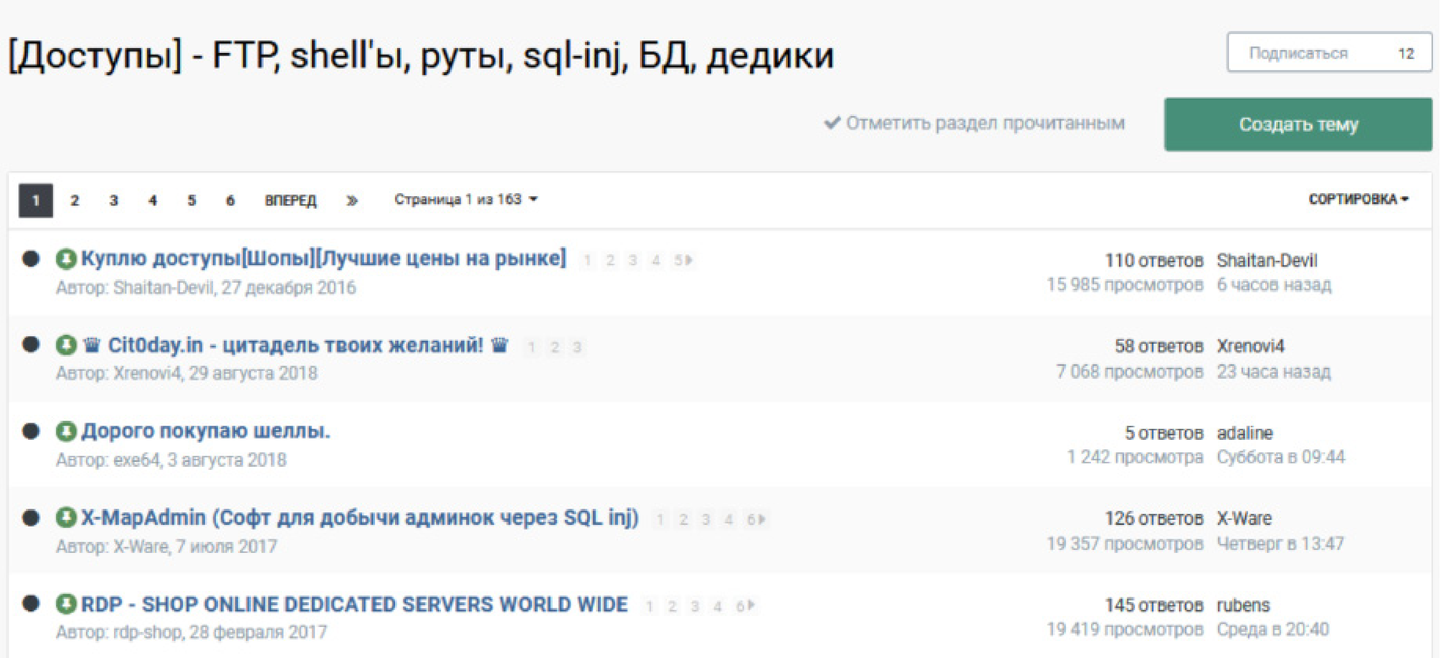
5. License to Extort: *Lowering the Barriers to Entry*

As we've seen, there are multiple ways for attackers to perform extortion attacks, whether they're looking to monetize leaked credentials, sensitive documents, intellectual property, or technical vulnerabilities. These methods require varying levels of time, resources, and sophistication on the part of the attacker, but time and again we see experienced or skilled attackers selling their knowledge or services to novices, such as with DoS- and ransomware-as-a-service models. And, as discussed in Digital Shadows' Tackling Phishing research, there's also an abundance of tutorials being traded on criminal forums, explaining techniques such as phishing. The extortion market is no less helpful, with the barriers to entry lower than they ever have been.

Access in the Market

For aspiring extortionists with weak skills, accessing your victims' machines and obtaining sensitive data to use for blackmail is one of the first—and potentially hardest—obstacles to overcome. Across many criminal forums, the overriding trend is for users to request "accesses" from each other: login details, credentials or sensitive files from a particular organization's or individual's machine.

Users of the more prestigious Russian-language criminal forums, in particular, have indicated their victims are overwhelmingly Western entities; offering accesses to victims in Russia or former Soviet countries is often seen as taboo or banned outright. The Exploit.in forum has a dedicated accesses section (Figure 8 below), and the Verified community has three sections where accesses are advertised and sourced. This isn't just a Russian or dark Web phenomenon, though. The English-language, surface Web platform Raidforums also has users trading accesses.



[Доступы] - FTP, shell'ы, руты, sql-inj, БД, дедики

● Куплю доступы[Шопы][Лучшие цены на рынке] 1 2 3 4 5
Автор: Shaitan-Devil, 27 декабря 2016
110 ответов 15 985 просмотров
Shaitan-Devil 6 часов назад

● ♛ Cit0day.in - цитадель твоих желаний! ♛ 1 2 3
Автор: Xrenovi4, 29 августа 2018
58 ответов 7 068 просмотров
Xrenovi4 23 часа назад

● Дорого покупаю шеллы.
Автор: exe64, 3 августа 2018
5 ответов 1 242 просмотра
adaline Суббота в 09:44

● X-MapAdmin (Софт для добычи админок через SQL inj) 1 2 3 4 6
Автор: X-Ware, 7 июля 2017
126 ответов 19 357 просмотров
X-Ware Четверг в 13:47

● RDP - SHOP ONLINE DEDICATED SERVERS WORLD WIDE 1 2 3 4 6
Автор: rdp-shop, 28 февраля 2017
145 ответов 19 419 просмотров
rubens Среда в 20:40

Figure 8: Dedicated accesses subsection of Exploit.in [Section titled: "[Accesses] - FTP, shells, roots, sql-inj, databases, dedicated servers", translated from Russian]

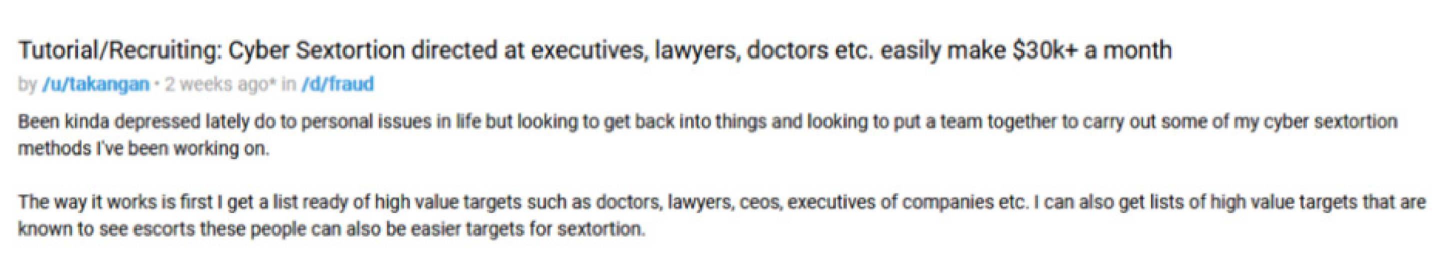
5. License to Extort:
Lowering the Barriers to Entry

Extortionists come in all shapes and sizes. We found admin panels, network and website access, and sensitive documentation peddled on the accesses sections of top-tier criminal forums. To best exploit these offers, buyers would need a high level of technical skills and the ability to move laterally inside victim networks, identifying the most suitable data for extortion.

At the other end of the scale, there is an active cybercriminal cracking scene in which entry-level buyers and sellers can share and trade vast sets of credentials and other accesses. The users of these forums would struggle to make use of the accesses commonly seen on sophisticated forums. However, access to compromised credentials can facilitate easier campaigns of the sextortion variety. Regardless of the attacker's sophistication, even an extortionist's claims of access would be enough to rattle some victims and coax them into complying with ransom demands.

Sextortion and the city

For threat actors requiring more than just help to acquire accesses and sensitive documents, there are always individuals offering to tutor or recruit apprentice extortionists. Sextortion-based attacks offer one of the easier entry routes for those fraudsters who are wet behind the ears. We've observed individuals on message boards and forums claiming that new recruits can make $30,000 or more through cyber sextortion scams directed at high-worth individuals, such as company executives and corporate lawyers (Figure 9).



Tutorial/Recruiting: Cyber Sextortion directed at executives, lawyers, doctors etc. easily make $30k+ a month

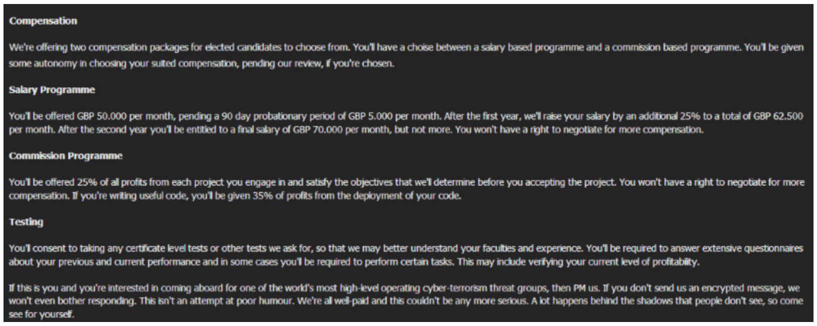
by /u/takangan · 2 weeks ago* in /d/fraud

Been kinda depressed lately do to personal issues in life but looking to get back into things and looking to put a team together to carry out some of my cyber sextortion methods I've been working on.

The way it works is first I get a list ready of high value targets such as doctors, lawyers, ceos, executives of companies etc. I can also get lists of high value targets that are known to see escorts these people can also be easier targets for sextortion.

Figure 9: Extract from sextortion tutorial and recruitment advertisement posted to online message board

For purer extortionists, the threat actor TDO used the KickAss forum to recruit individuals with network management, penetration testing, and programming skills. TDO posted job advertisements with specifications and salaries that would rival those offered by most corporate businesses. Recruits were tempted with £50,000 ($64,000) per month, with add-ons and a final salary after the second year of £70,000 ($90,000) per month (Figure 10). Those with Chinese, Arabic or German skills could earn an added five percent on their salary or commission.



Compensation

We're offering two compensation packages for elected candidates to choose from. You'll have a choise between a salary based programme and a commission based programme. You'll be given some autonomy in choosing your suited compensation, pending our review, if you're chosen.

Salary Programme

You'll be offered GBP 50.000 per month, pending a 90 day probationary period of GBP 5.000 per month. After the first year, we'll raise your salary by an additional 25% to a total of GBP 62.500 per month. After the second year you'll be entitled to a final salary of GBP 70.000 per month, but not more. You won't have a right to negotiate for more compensation.

Commission Programme

You'll be offered 25% of all profits from each project you engage in and satisfy the objectives that we'll determine before you accepting the project. You won't have a right to negotiate for more compensation. If you're writing useful code, you'll be given 35% of profits from the deployment of your code.

Testing

You'll consent to taking any certificate level tests or other tests we ask for, so that we may better understand your faculties and experience. You'll be required to answer extensive questionnaires about your previous and current performance and in some cases you'll be required to perform certain tasks. This may include verifying your current level of profitability.

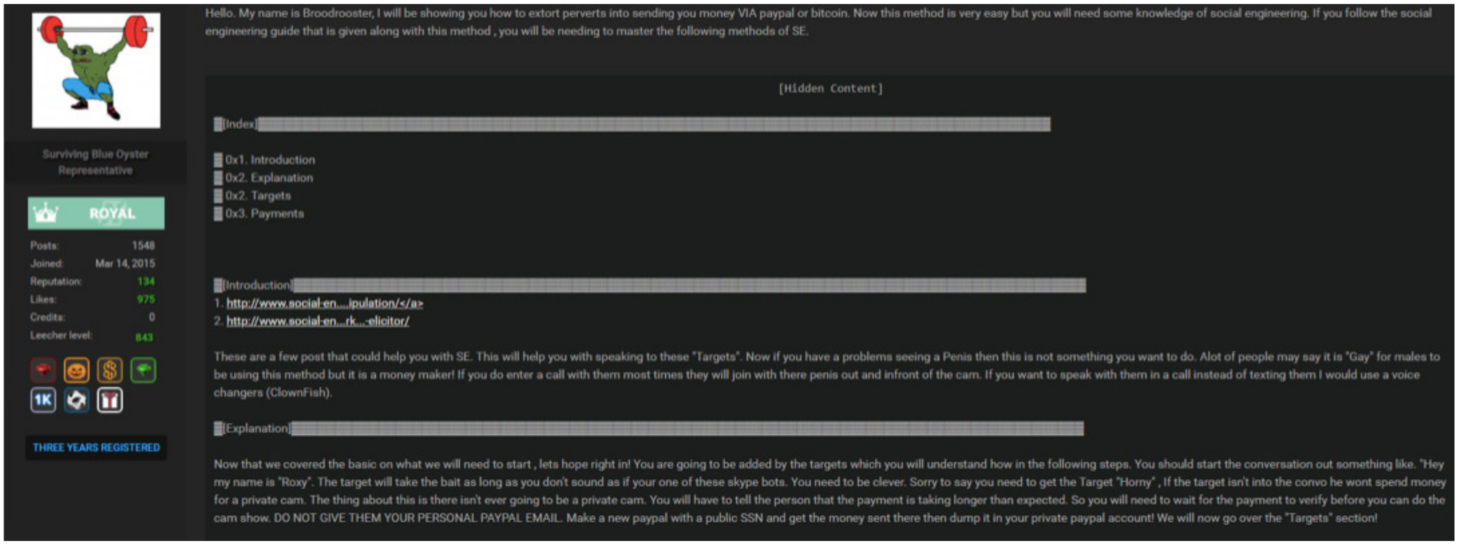
If this is you and you're interested in coming aboard for one of the world's most high-level operating cyber-terrorism threat groups, then PM us. If you don't send us an encrypted message, we won't even bother responding. This isn't an attempt at poor humour. We're all well-paid and this couldn't be any more serious. A lot happens behind the shadows that people don't see, so come see for yourself.

Figure 10: TDO recruitment post on KickAss

5. License to Extort:
Lowering the Barriers to Entry

Extortion guides for sale

Those wanting to go it alone have no shortage of options to get started, with blackmail and extortion guides advertised on criminal forums. In Figure 11 a user on the Nulled forum is offering a sextortion guide whereby the threat actor poses online as a woman to encourage men to send compromising photos of themselves. Similar guides are available on dark web marketplaces such as Dream Market for less than $10. One of these guides, obtained by Digital Shadows, specifically focuses on a sextortion tactic whereby the threat actor begins an online relationship with a married man and then threatens to reveal details of the affair with his partner unless a ransom is paid. The guide claims this extortion method is the easiest for novice threat actors to start with, suggesting they could earn between $300-500 per extortion attempt.



Surviving Blue Oyster Representative

Posts: 1548
Joined: Mar 14, 2015
Reputation: 134
Likes: 975
Credits: 0
Leecher level: 843

Hello. My name is Broodrooster, I will be showing you how to extort perverts into sending you money VIA paypal or bitcoin. Now this method is very easy but you will need some knowledge of social engineering. If you follow the social engineering guide that is given along with this method , you will be needing to master the following methods of SE.

[Hidden Content]

[Index]

0x1. Introduction
0x2. Explanation
0x2. Targets
0x3. Payments

[Introduction]

1. http://www.social-en....ipulation/</a>
2. http://www.social-en...rk...-elicitor/

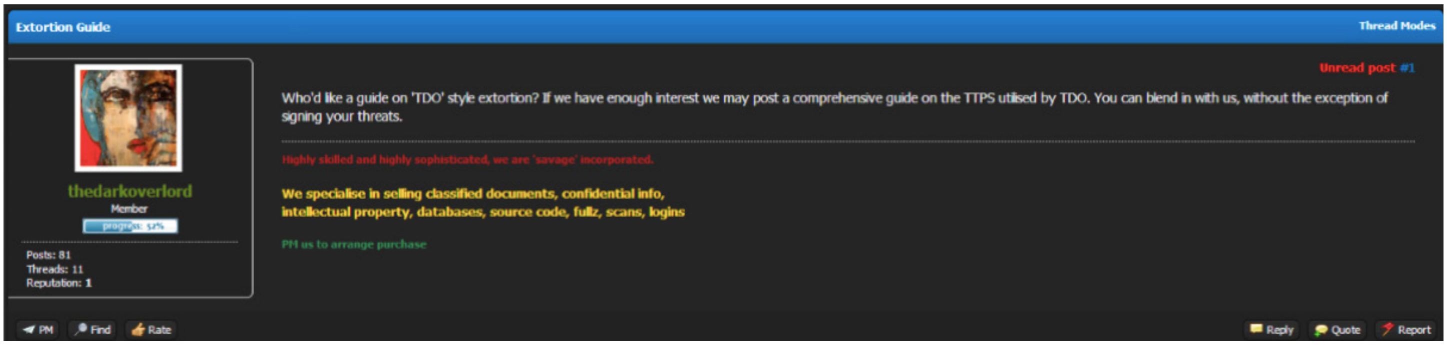
These are a few post that could help you with SE. This will help you with speaking to these "Targets". Now if you have a problems seeing a Penis then this is not something you want to do. Alot of people may say it is "Gay" for males to be using this method but it is a money maker! If you do enter a call with them most times they will join with there penis out and infront of the cam. If you want to speak with them in a call instead of texting them I would use a voice changers (ClownFish).

[Explanation]

Now that we covered the basic on what we will need to start , lets hope right in! You are going to be added by the targets which you will understand how in the following steps. You should start the conversation out something like. "Hey my name is "Roxy". The target will take the bait as long as you don't sound as if your one of these skype bots. You need to be clever. Sorry to say you need to get the Target "Horny" , If the target isn't into the convo he wont spend money for a private cam. The thing about this is there isn't ever going to be a private cam. You will have to tell the person that the payment is taking longer than expected. So you will need to wait for the payment to verify before you can do the cam show. DO NOT GIVE THEM YOUR PERSONAL PAYPAL EMAIL. Make a new paypal with a public SSN and get the money sent there then dump it in your private paypal account! We will now go over the "Targets" section!

Figure 11: Blackmail guide advertised on Nulled

TDO also used the KickAss forum to advertise extortion guides, priced at BTC 5 (Figure 12). The guide allegedly contained over 200 pages of content and advice, detailing the threat actor's extortion TTPs.



Extortion Guide

thedarkoverlord
Member
progress: 52%

Posts: 81
Threads: 11
Reputation: 1

Who'd like a guide on 'TDO' style extortion? If we have enough interest we may post a comprehensive guide on the TTPS utilised by TDO. You can blend in with us, without the exception of signing your threats.

Highly skilled and highly sophisticated, we are 'savage' incorporated.

We specialise in selling classified documents, confidential info, intellectual property, databases, source code, fullz, scans, logins

PM us to arrange purchase

Figure 12: TDO offering extortion guide on KickAss

6. Avoiding the Shakedown: *Reduce Your Extortion Risks*

While extortion techniques diversify and the market is more accessible than ever, we're not making it any easier on ourselves by failing to manage our online exposure effectively. As we've seen, extortionists take advantage of millions of compromised credentials circulated on forums, paste sites, and public channels. Meanwhile, your attack surface may be left wide open from not patching publicly known and exploitable vulnerabilities on your Internet-facing applications. In short, you could be making the jobs of extortionists like SamSam easier than taking candy from a baby.

Minimizing online exposure

Luckily, as consumers and businesses, we have a large amount of control over whether we will be the victims of an extortion attempt. To reduce your extortion risks, begin by focusing on identifying and minimizing your online exposure in the following ways.

Stop account takeover dead in its tracks

1. Enable multi-factor authentication (MFA), where possible, to help prevent account takeovers and minimize risk even if your password is leaked publicly.
2. Use strong passwords generated from a password manager like 1Password or LastPass.
3. Don't reuse passwords, especially for privileged accounts.
4. Use unique local administrator passwords. Although time-consuming to deploy, products such as Microsoft Local Administrator Password Solution (LAPS) can help you manage local account passwords.
5. Use such services as Have I Been Pwned? to check whether your credentials have been leaked publicly.

Combat sensitive data loss

1. Regularly back up data in case of catastrophic loss, and store sensitive files in detached storage away from the main network. Critically, don't forget to periodically test your back-up and recovery processes. The wrong time to identify flaws in your disaster recovery strategy is after all your critical data has been encrypted.
2. Safeguard important data by only granting access to those who have a business requirement for it. Also practice the principle of least privilege, reducing the number of users who have access to important data if an attacker gains access to your network.
3. Ensure cloud storage solutions and file sharing services, such as anonymous FTP, SMB and rysnc, are properly configured to prevent accidental file exposure.
4. Be aware of, and provide training on, the risks posed by employees and contractors who back up files on network-attached storage (NAS) devices. Users should add a password and disable guest/anonymous access, as well as opt for NAS devices that are secured by default. Ideally, offer back-up solutions so employees don't feel the need to back up their devices at home.

6. Avoiding the Shakedown: *Reduce Your Extortion Risks*

Shrink your attack surface

1. Go through the process of discovering which protocols or features are explicitly required for a system to function. Disable all other legacy or unnecessary features to harden your system against attack.
2. Create an inventory of software and services connected to the public-facing Internet to prioritize patching.
3. Apply vendor patches in a timely fashion to reduce the number of exploitable vulnerabilities in installed software as part of a continuous vulnerability assessment program.
4. Ideally, make remote-access solutions (such as RDP) accessible only over a VPN. Where not possible, use access control lists to restrict which IP address ranges can connect to the service
5. Aggressively prevent and filter BYOD (bring your own device) with missing (security) patches from accessing resources in the network.

Handling sextortion emails

These scams are generally mass, opportunistic campaigns that rely on a target list large enough that the operators will continue to receive payments. Users should ignore these emails, but also stay vigilant and inspect their inbox more closely. Look out for the telltale signs that you are being targeted by a mass scam campaign. If such messages are making their way into your corporate inbox, speak to your IT teams, who can reevaluate email filtering controls.

Additional security measures such as Sender Policy Framework (SPF), Domain-based Message Authentication, Reporting And Conformance (DMARC) and DomainKeys Identified Mail (DKIM) can be used to combat email spoofing attempts, which are commonly used by spammers. For more detail on email spoofing, check out our Security Practitioner's Guide to Email Spoofing and Risk Reduction.

The FBI's Internet Crime Complaint Center (IC3) accepts complaints from the public regarding scams like sextortion. Since there is significant overlap between personal and business lives, firms should educate their staff on the latest sextortion campaigns.

6. Avoiding the Shakedown: *Reduce Your Extortion Risks*

Readying for ransomware

To prevent general ransomware variants, regularly back up files away from the corporate network or an external device to help mitigate data loss. Businesses should also develop and practice from a ransomware playbook so that all staff (operations, IT, security, legal, PR) know their role if trouble hits.

Simulating SamSam

The SamSam group has made use of a variety of open-source tools, listed below for you to use in your purple team security assessments (which should be part of an ongoing process to evaluate your own controls).

- JexBoss
  (CVE-2010-0738 exploit)
- NLBrute v1.2
  (WARNING: hacker tool,
  download at your own risk!)
- PowerSploit
- PsExec
- PsInfo
- Hyena
- Mimikatz

The moral of the tale

Often, discussions around cybersecurity risks and threats can seem obscure and of little relevance to the majority of individuals and organizations. Extortion, on the other hand, has a particularly strong human element. The results of an extortion attempt can be particularly damaging for victims. SamSam has targeted healthcare organizations and the public sector, where the disruption or loss of data caused by a ransomware attempt has far-reaching consequences for all those that rely on those services. Likewise, mass opportunistic sextortion campaigns can leave individuals both out of pocket and in emotional distress.

The threat of extortion can therefore seem intimidating and, in many senses out, of our control. What this paper shows, however, is that extortionists are often dependent and enabled by our own inability to properly manage our digital footprints. If we look at it this way, then reducing extortion becomes a much more manageable process, and one that we can feel more confident about combating.

Ransom (End)Notes

1. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-asaftd
2. https://www.digitalshadows.com/blog-and-research/thedarkoverlord-out-to-kickass-and-cash-out-their-data/
3. https://www.digitalshadows.com/blog-and-research/thedarkoverlord-losing-his-patients/
4. https://motherboard.vice.com/en_us/article/gv5dzq/the-administrator-of-the-dark-webs-infamous-hacking-market-the-real-deal-has-vanished
5. https://www.digitalshadows.com/blog-and-research/crowdsourced-ddos-extortion-a-worrying-development/
6. https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public
7. https://blog.talosintelligence.com/2016/03/samsam-ransomware.html
8. https://blog.malwarebytes.com/cybercrime/2018/05/samsam-ransomware-need-know/
9. https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-ransomware-chooses-Its-targets-carefully-wpna.pdf
10. https://www.us-cert.gov/ncas/current-activity/2018/09/28/IC3-Issues-Alert-RDP-Exploitation
11. https://attack.mitre.org/wiki/Main_Page
12. https://www.digitalshadows.com/blog-and-research/tackling-phishing-the-most-popular-phishing-techniques-and-what-you-can-do-about-it/

About Digital Shadows

Digital Shadows minimizes digital risk by identifying unwanted exposure and protecting against external threats. Organizations can suffer regulatory fines, loss of intellectual property, and reputational damage when digital risk is left unmanaged. Digital Shadows SearchLight™ helps you minimize these risks by detecting data loss, securing your online brand, and reducing your attack surface.

To learn more and get free access to SearchLight, visit www.digitalshadows.com.

London

Columbus Building, Level 6,
7 Westferry Circus,
London, E14 4HD

+44 (0) 203 393 7001

messages@digitalshadows.com

San Francisco

332 Pine St. Suite 600,
San Francisco, CA 94104

+1 (888) 889 4143

Dallas

5307 E. Mockingbird Ln.
Suite 200
Dallas, TX 75206

digital shadows_