



14 | 0 | 1 | 1 | 1 | 1 | 1 | 5 | 0 | 1 | 1 |

Pay up or else...

Cyber Ransom Survival Guide

*The Growing Threat of Ransomware
and RDoS - and What to Do About It*

Table of Contents

01 Introduction

02 Current Threat Environment

03 RDoS: Attackers and Their Targets

04 Beware the RDoS Copycats

05 Likely Targets: Will You CAVE?

06 Targets by Industry

07 Cyber Ransom Marketplace

08 Be Prepared: Key Questions and Actions

09 Cyber Ransom Lexicon

01

Introduction

It's 9:30 in the morning. You've grabbed your morning coffee and caught up on email. Now you're settling in to read an article online. Suddenly, your machine freezes, and this message pops up:

“You have been caught accessing inappropriate content and your device will remain locked unless you pay \$\$\$\$.”



Welcome to the world of cyber ransom—one of the fastest-growing security concerns around the globe. At its root, the concept is hardly novel; blackmail has been around for ages. Today it has morphed into some decidedly modern and malicious varieties:



Ransomware

A Trojan, worm or other form of malicious software takes an environment hostage by making it unavailable to use unless a payment is made. The most common forms totally encrypt the environment and require payment to decrypt. However, there are numerous other tactics being deployed that focus on availability of systems and data.



Ransom Denial of Service (RDoS)

In an RDoS attack, the perpetrators send a letter threatening to attack an organization—rendering its business, operations or capability unavailable—unless a ransom is paid by the deadline. These attacks have grown in number every year since 2010 and typically come in the form of a volumetric distributed denial-of-service (DDoS) attack. However, it is increasingly in vogue to find techniques that are more piercing and more efficient without generating large volumes. The most advanced attacks combine both volume and non-volume cyberattack techniques.

Every day, ransom tactics are being used to target individuals and companies across industries around the world. The potential harm can be devastating. Other types of attacks, such as advanced persistent threats or multi-layer attacks, take a long time to defend against or even to detect. By contrast, ransomware and RDoS threats shout, “I’m an attack and I’m right here!” You then have 24 to 48 hours to pay the ransom or suffer the loss.

What can you do about cyber ransom? As with so many threats, knowledge is power. This e-book offers a concise overview of the topic—including the current threat landscape (with samples of actual letters and tweets), who’s likely to be targeted (and why), the marketplace and tools fueling the trend and, perhaps most importantly, questions you need to ask and steps you need to take to safeguard your organization. At the end of the e-book, you’ll find a lexicon of related terms to help you speak the “language” of cyber ransom.

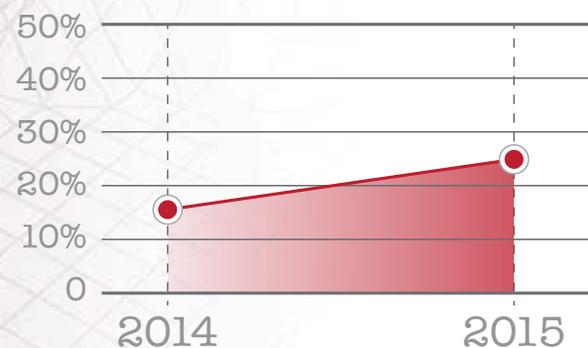
So, grab another cup of coffee and get ready to learn about one of the fastest-growing threats to the security of your business...

02

Current Threat Environment

Motivation: Ransom

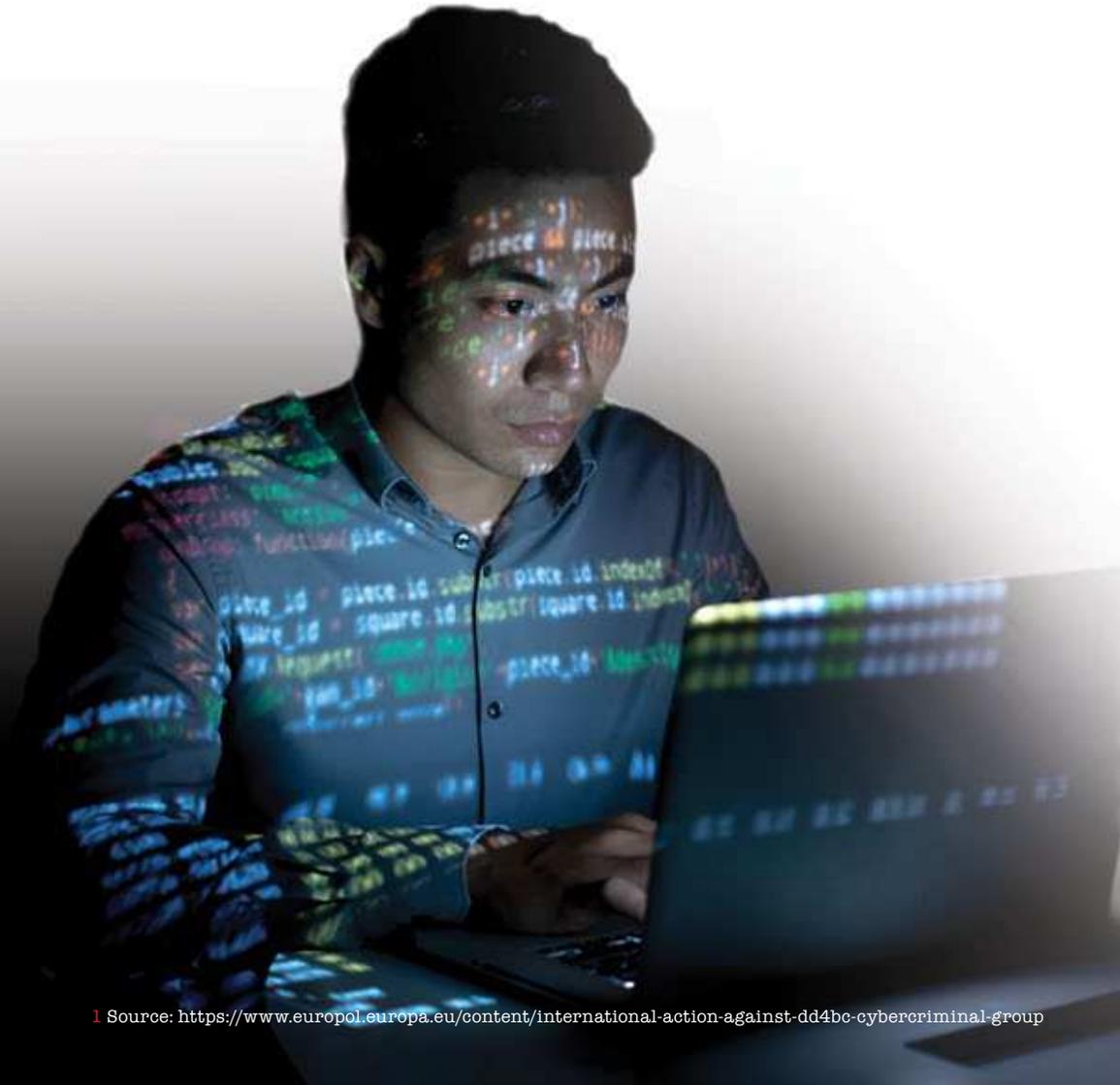
As Radware reported in its *2015-2016 Global Application & Network Security Report*, ransom as a motivation for attackers is on the rise—accounting for 16% of attacks in 2014 and 25% in 2015. What's driving the increase? Quite simply, it's getting faster, easier and cheaper to execute these attacks. A growing marketplace offering cyber ransom tools and techniques is arming everyone from college students to organized hacker groups with the resources they need to facilitate attacks—and turn quick profits. Meanwhile, it's getting easier to mask the source of attacks. Attackers can spoof IPs or access targets via a content delivery network (CDN) or global network address translation (NAT), thereby concealing the specific resources launching an attack within a broader network.



Source: 2015-2016 Global Application & Network Security Report

03

RDoS: Attackers and Their Targets



To date, RDoS attacks have been carried out primarily by these groups:

DD4BC

This cybercriminal group, whose name is an acronym for distributed denial of service for Bitcoin, started launching Bitcoin extortion campaigns in mid-2014. Initially targeting the online gambling industry, DD4BC has since broadened targets to include financial services, entertainment and other high-profile companies.¹

Armada Collective

Another gang of cybercriminals, Armada Collective uses tactics similar to DD4BC and typically demands a ransom of 10 to 200 BTC (about US\$3,600 to US\$70,000). This gang is known for accompanying its ransom notes with a short “demo” attack. When time for payment expires, Armada Collective takes down the victims’ data centers with traffic volumes typically exceeding 100Gbps. Radware has firsthand experience with these criminals, who waged an RDoS attack against its customer, ProtonMail, in 2015. Subsequently, apparent copycats began using the Armada Collective name; one early tactic involved attempted extortion of about US\$7.2 million from three Greek banks.

¹ Source: <https://www.europol.europa.eu/content/international-action-against-dd4bc-cybercriminal-group>

ezBTC Squad

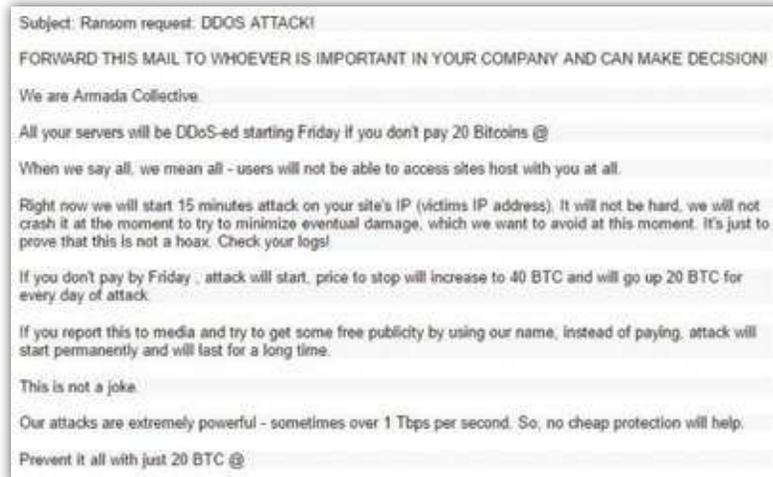
Instead of using email messages, this group of cybercriminals is using Twitter as the vehicle for delivering its RDoS threats. Others are following suit.

Kadyrovtsy

Named after the elite forces of the Kadyrov administration in Chechnya, this is one of the newest groups to emerge on the RDoS scene. It recently threatened two Polish banks and a Canadian media company. The group even launched demo assaults (15-20 Gbps) to prove its competence, much like the infamous Armada Collective.

RedDoor

RedDoor issued its first threats in March 2016. Per the “standard,” these criminals use an anonymous email service to send messages demanding a ransom of 3 Bitcoins. Targeted businesses have just 24 hours to wire the payment to an individual Bitcoin account.



Subject: Ransom request: DDOS ATTACK!

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

All your servers will be DDoS-ed starting Friday if you don't pay 20 Bitcoins @

When we say all, we mean all - users will not be able to access sites host with you at all.

Right now we will start 15 minutes attack on your site's IP (victims IP address). It will not be hard, we will not crash it at the moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a hoax. Check your logs!

If you don't pay by Friday, attack will start, price to stop will increase to 40 BTC and will go up 20 BTC for every day of attack.

If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long time.

This is not a joke.

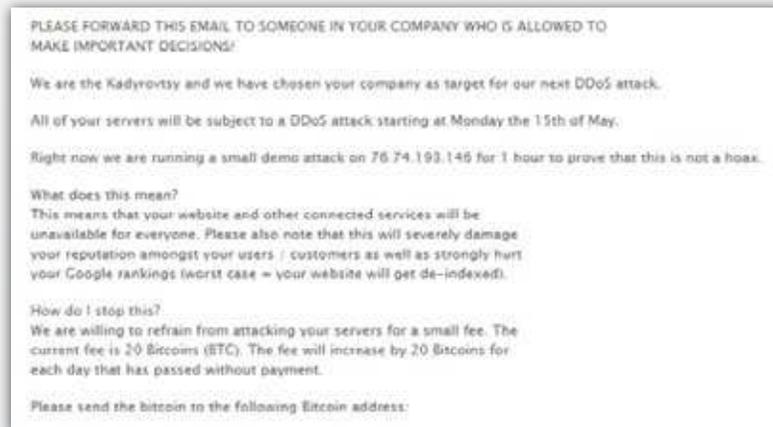
Our attacks are extremely powerful - sometimes over 1 Tbps per second. So, no cheap protection will help.

Prevent it all with just 20 BTC @

Figure 1. Sample ransom letter from Armada Collective.



Figure 2. Ransom tweet from EzBTC Squad.



PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS!

We are the Kadyrovtsy and we have chosen your company as target for our next DDOS attack.

All of your servers will be subject to a DDOS attack starting at Monday the 15th of May.

Right now we are running a small demo attack on 76.74.193.145 for 1 hour to prove that this is not a hoax.

What does this mean?

This means that your website and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation amongst your users / customers as well as strongly hurt your Google rankings (worst case = your website will get de-indexed).

How do I stop this?

We are willing to refrain from attacking your servers for a small fee. The current fee is 20 Bitcoins (BTC). The fee will increase by 20 Bitcoins for each day that has passed without payment.

Please send the bitcoin to the following Bitcoin address:

Figure 3. Sample ransom letter from Kadyrovtsy.

A group of hooded figures in a city at night, with binary code overlaid on the image. The central figure is a man with a serious expression, looking directly at the camera. The background shows a city skyline with lights. The text '04' is prominently displayed in the lower-left corner.

04

Beware the RDoS Copycats

“Copycats” are compounding the RDoS headaches. These players are issuing fake letters—hoping to turn quick profits with minimal effort. How can you detect a fake ransom letter?

Assess the Request.

The Armada Collective normally requests 20 Bitcoin. Other campaigns have been asking for amounts above and below this amount. Fake hackers request different amounts of money. Low Bitcoin ransom letters are most likely from fake groups who are hoping their price point is low enough for someone to pay rather than seek help from professionals.

Check your Network.

Real hackers prove their competence by running a small attack while delivering a ransom note. If you can see a change in your network activity, the letter and the threat are probably genuine.

Look for Structure.

Real hackers are well organized. Fake hackers, on the other hand, don't link you to a website. Nor do they have official accounts.

Consider Other Targets.

Real hackers tend to attack many companies in a single sector. Fake hackers are less organized, targeting anyone and everyone in hopes of making a quick buck.

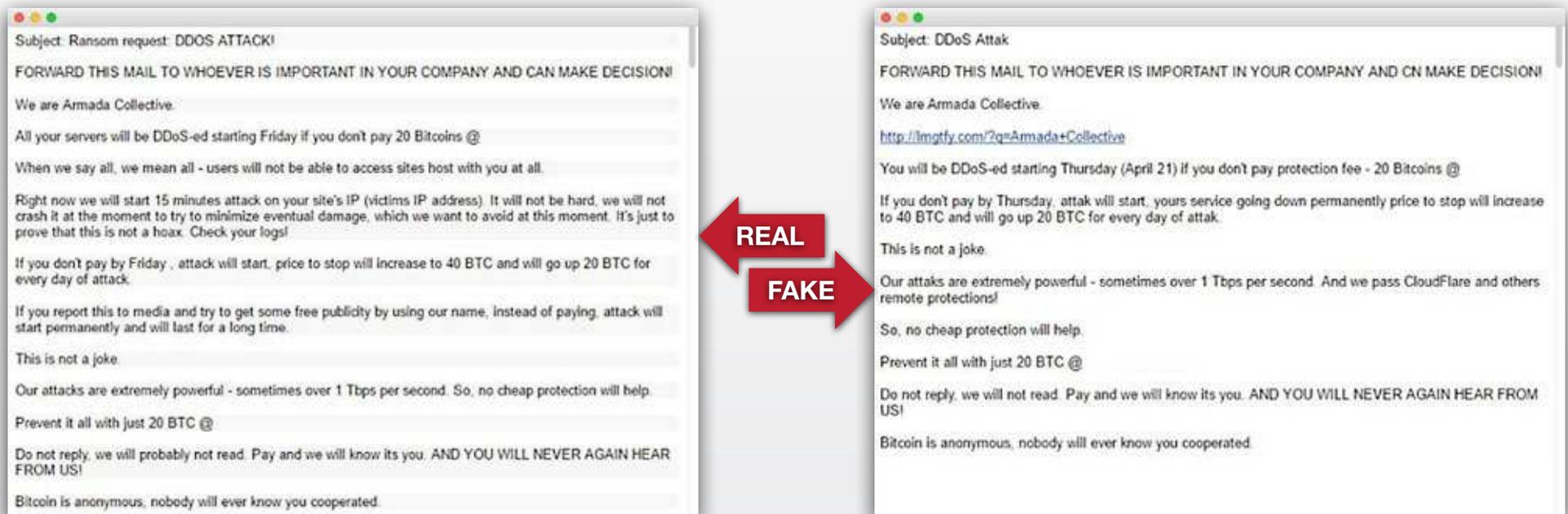


Figure 4: Samples real and fake ransom letters.

Ransomware

Ransomware isn't new—it's been on the scene for nearly a quarter century. One of the first examples was called Aids Info Disk or PC Cyborg Trojan. This Trojan horse would encrypt all of the filenames on the "C" drive—rendering the PC unusable. Once a PC was infected, the ransomware would demand that a payment of \$189 be sent to a post office box somewhere in Panama. In time, the Aids Info Disk Trojan's creator was arrested and charged with 11 counts of blackmail.

In time, antivirus software makers learned how to detect this category of malware and were able to quickly block them. For years, their techniques worked. However, the growing popularity of virtual currencies have made ransomware a potentially lucrative opportunity for cyber criminals. No one is requesting payments to a PO box; these days, victims are told that if they ever want to see their information again, they must make a payment to a hacker via Bitcoin. Of course, the only sure thing is that the money will be taken.

Ransomware-as-a-Service

New types of ransomware are cropping up quickly—taxing antivirus software providers' ability to keep pace. The latest threat is Ransom32, ransomware-as-a-service. Rather than building his or her own software, the potential cybercriminal pays a fee to customize and use this ready-made ransomware platform. Profits are shared by the platform developer and the ransomers who use the platform to execute campaigns. The scariest part? Expert skills are no longer required to hold a victim's information hostage.

Not Just PCs

Ransomware has branched out beyond Windows PCs to infect Android mobile devices and even Network-attached storage (NAS) devices. In recent months, nearly 300 new malware variants that affect Android devices have been detected. What's more, highly specialized ransomware—designed to encrypt the information stored on a Synology NAS—began to attack. By exploiting a vulnerability in the device's software, the ransomware has been able to take control of the stored information.

Evolving Toolset

While some of the early ransomware tools extorted individuals, new tools are targeting businesses in hopes of a greater financial gain. New variants are already posing operational and financial challenges to numerous businesses. Such tools encrypt all files on a certain server or workstation, which can be decrypted and restored only if the ransom is paid to the attacker.

- **Locky** propagates through spam emails with infected files, and changes all file extensions to .locky.
- **Samas** exploits webserver's vulnerabilities to spread inside the network.
- **Petya** propagates via phishing and introduces a new method of overriding hard drive MBR.
- **Cerber** masquerades itself as an Adobe Flash player update, impersonating a Windows executable to pop up in the next reboot.
- **BART** an evolution of Locky and from the same creators, distributed through spam email after locky has become well known. BART does not encrypt the files, but creates a password protected archive.
- **CTB Locker** spreads via customized deceptive emails. It can encrypt several machines within the same network, and also features a mechanism of recognizing malware analysis programs in order to avoid them (it simply won't be triggered).
- **CryptXXX** spreads via spam emails. Scans files and adds the .crypt extension. 2.0, 3.0. and 4.0 versions feature immunity against free decryption tools, thus more victims tend to pay the ransom.
- **Unlock 92** using RSA-2048 algorithm to encrypt files. Communicates in Russian only. In many cases did not unlock the files though payment was received.
- **TeslaCrypt** typically exploits Adobe vulnerabilities and uses an AES algorithm to encrypt files.
- **Jigsaw** after encrypting the files, begins deleting them in bulks every hour until the ransom is paid (or all at once after 72 hours).



Figure 5. Locky ransomware toolset.



Figure 6. Petya ransomware toolset.



Figure 7. Cerber ransomware toolset.

05

Likely Targets: Will You CAVE?

What do cyber criminals look for when considering ransom targets? The acronym CAVE highlights the four areas criminals will assess when choosing which people and companies to target:

Culture.

An organization's culture can make it more or less likely to be targeted by cyber criminals. The two key factors: cultural views on paying vs. not paying and the organization's overall appetite for risk. Some organizations are afraid to go public about a breach or simply aren't interested in a public "fight." Very private, risk-averse organizations may represent strong candidates for an RDoS or ransomware attack. Similarly, those with a pay-up culture—who are quick to send funds to "make it go away"—often earn a reputation as such. That can result in new attacks from other cyber-crime groups.

Assets.

Clearly, there must be some digital asset—business or personal data, interface or communication—that is critical to an individual's life or an organization's operations. Those digital assets are what the criminals will attempt to hold hostage.

Case Study: Payment Processor

This payment processor touches a significant number of American consumers—processing some 60 to 70 percent of the nation’s PIN transactions. For years, its operations ran smoothly and successfully, with little cause for concern around information security. That all changed a few months into 2015, when it received a “pay up or else” letter from cyber-attackers demanding ransom money. In time, the company learned it was among a number of payment-processing companies receiving such letters. Though the victims seemed somewhat random, similarities among the letters suggested at least a loosely organized campaign.

The perpetrators—who likely will never be identified or brought to justice—waged what amounted to the modern-day equivalent of neighborhood thugs shaking down merchants for protection money. The threat tactics underscored that DDoS attacks are a viable weapon for extortion—and that no industry, no company, no country is immune. Even firms that keep an intentionally low profile online, as this processor had, can become targets.

With no experience managing such a threat, the company engaged Radware for emergency support. Radware quickly spun up its Emergency Response Service, offering a service-based model for protecting the company’s critical systems. Since the company chose not to respond to the ransom threats, its systems were placed under attack. Thanks to Radware’s support, it had a strong defense—and the attacks did not impact its operations or customers.

Vulnerability.

Cyber criminals need a way to lock down assets, making them unavailable to users. In general, they can do so in two primary ways: either by encrypting data at some level or by denying access by taking hostage an element of the information technology delivery chain. Either way, criminals need to spot a key vulnerability—such as an exploit or engineering assumption left unprotected. Ideally, cyber criminals will seek vulnerabilities that are present across a large number of organizations. Such vulnerabilities can be highly lucrative, giving criminals the ability to standardize on a technique and repeat it on a mass scale.

Expertise.

Strictly speaking, criminals aren’t looking for expertise; they’re looking for a lack of it. They’re more likely to focus on organizations or people lacking the resources to hire professionals; those with few or modest investments in IT security support; and those who lack knowledge of cyber-ransom techniques and how best to respond.

06

Targets by Industry

How does the CAVE criteria translate into actual targets? In other words, which industries and people have shown themselves as being vulnerable to these attacks? Radware observation, experience and analysis point to the following:

Financial Advisors and Financial Services Companies.

This industry evokes the old joke: Why do criminals rob banks? Because that's where the money is. Cyber criminals are no different; they frequently go to the source of money or to those have access to it.

Hospitals and Other Healthcare Organizations.

Hospitals seem to fall firmly at one end of the spectrum or the other. Some are aligned toward paying up; others are principally resolute and driven NOT to pay a ransom.



Attorneys and Law Firms.

Law firms aren't known for investing large sums in security. In most cases, they aren't adroit at internal controls, either. Yet firms are highly dependent on their ability to create and share information. What's more, they're notoriously hesitant to go public with a breach, fearing that their typically high-profile client base would be shaken. Add it all up, and you have an industry segment that's very likely to be targeted—and to capitulate.

Professional Services Firms.

Much like law firms, accounting, architectural, consulting and other professional services companies may be afraid to go public with a breach. This unwillingness to engage in public discourse makes these firms more likely to be targeted—and to pay up.

Schools and Educational Services.

Ironically, educational institutions typically aren't savvy in information security and cyber-attack mitigation. Even if they have the expertise, they may lack the financial means to wage a protracted war with a cyber-ransom group. In addition, schools often make decisions by committee—making them more prone to pay up rather than stick to firm, universal principals.

Manufacturing and the IoT.

Concerns about the Internet of Things (IoT) and manufacturing attacks could be the Valhalla of cyber ransom. After all, who wouldn't pay up to regain access to their car, home thermostat or, even worse, the defibrillator that regulates the beat of their heart? Though mere conjecture today, the risks of IoT-related cyber ransom—particularly associated with human health—are far too compelling to rule out.

Clashing Ideologies

Any organization that's already under scrutiny by one or more activist groups should assume that those clashes could eventually spill into criminal activity—including cyber ransom. What follows is a sampling of the types of activities and affiliations that could make an organization vulnerable:

- Animal cruelty, testing or hunting
- Anti-LGBT
- Federal, state or local law enforcement
- Genetic or industrial farming
- Firearms or defense
- Politicians, actors, musicians and other public figures
- Fossil fuel industry (oil, gas, petrochemical)
- Religious affiliations

Getting Personal

In addition to the industries and organizations cited above, there are some very personal attributes that may dramatically increase the risk of a cyber-ransom incident.

College students are famous for their lack of funds and urgent need for instant access to their “stuff.” Lack of patience and insufficient knowledge addressing technical attacks make this group ripe for paying up and other forms of capitulation.

Politicians, actors and other public figures typically have far greater financial resources than college students. However, when under attack, this group typically prefers not to endure the public scrutiny that an aggressive response would require.

Finally, corporate officers have long been the targets of death threats, as well as physical and verbal attacks. Cyber ransom is the latest way to come after big-company leaders. Unfortunately, a company’s resources for fighting an attack may outlast an individual’s ability to withstand the heat—leading the corporate officer to give in to the cyber criminals.



07

Cyber Ransom Marketplace

BUY NOW

Ransomware

DDoS Attack

Botnets

Exploits

You can order just about anything via the Internet—and cyber ransom tools and services are no exception. The entry point for cyber attackers keeps dropping, as more vendors rush to sell their services both on the Darknet and the Clearnet.

Attackers can now easily purchase a number of service—from undisclosed exploits and malware to botnets, bulletproof hosting and other attack services. Even an attacker with limited skill can purchase full-service items that offer setup assistance for botnets and ransomware campaigns. Sadly, an attacker wishing to leverage cyber-ransom tools is limited only by his or her budget. Those who can afford them can gain instant access to some of the more sophisticated tools available today.

On a nearly daily basis, vendors advertise their services on Twitter or other social networks. These ads are typically accompanied by a link either to a forum where the services can be purchased or to a paste site with additional information about the services and how to procure them.

text 0.60 kb raw download clone embed report print

1. **Want to buy DDoS from us? Just download Tor Browser Bundle from <http://torproject.org/> - create an alphabay account at <http://pwoah7foa6au2pu1.onion/> - buy some bitcoin from <http://coinbase.com/> or <http://localbitcoins.com> - put bitcoin in AlphaBay account - order DDoS from us via our listing available on our vendor account: <http://pwoah7foa6au2pu1.onion/user.php?idevproducts>**
2. **You can also manually purchase by adding us on XMPP at hdmi@swissjabber.ch - Google how to use Pidgin and create a Jabber account.**
3. **If you want premium DDoS, you will put in the work to get it securely. Our competitors are no match!**

Figure 8. Sample ad from [XXX?].

The Cyber-Ransom ‘Catalog’

What, exactly, can be bought? “Merchandise” changes frequently, but at present, the offerings fall into four high-level categories: botnets, DDoS attacks, exploits and ransomware. Here’s a brief overview on each.

Botnets

Botnet services are commonly found on both the Clearnet and the Darknet. Would-be attackers can purchase anything from tutorials on how to control and deploy their own to the malware itself. If purchasers don’t care to learn how to deploy the botnet, they can buy a setup service or even rent someone’s botnet temporarily. The average rental cost for a large botnet ranges from .025 BTC – .05 BTC (\$16.79 – \$ 33.79) per hour. The malware itself can sell for hundreds, sometimes thousands, of dollars. Among the main functions these bots offer: DDoS attack via UDP, TCP, GET and POST floods, along with the ability to emulate and bypass some JavaScript and cookie challenges.

Vim's Fraud Store
@vimproducts

To buy DDoS (server stress testing) or other services from us, go here:
pastebin.com/yhiYD3hZ

2:08pm · 30 Apr 2016 · Twitter Web Client

Figure 9. Sample Twitter as for cyber-ransom tools.

BHGroup full botnet setup A to Z

*** This listing is non-refundable *** please read the description completely before buying the listing. this service is not recommended for low budget individuals. currently there is so such a service in deep web nor clearnet ! what is this service : this listing is for individuals who are interested to own a botnet for a lot of reasons, this service will help you to choose best b...

Sold by BHGroup - 9 sold since Dec 18, 2015 Vendor Level 4 Trust Level 4

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Figure 10. Sample of a botnet for purchase.

DDoS Attacks

While DDoS attacks can be purchased both on the Clearnet or the Darknet, a large majority can be found on the Clearnet being sold as booter or stresser services. Notorious DDoS groups, such as Lizard Squad, run their own public DDoS services. Lizard Squad's current service is called Shenron. Shenron offers eight packages ranging from as little as \$19.99 to as much as \$999.99 a month. Attack times for these packages range from 1,200 to 18,000 seconds of boot time, with power allegedly ranging from 35Gbps to 500Gbps. Shenron's services currently offer three different attack methods: DNS, SNMP and SSYN.

Exploits

Darknet marketplaces often offer a number of exploit codes for sale. Examples could include a local privilege escalation on Windows 8.1 or a single message DoS exploit on Telegram. Attackers can also find exploits, such as a Remote Code Execution (RCE) that allows upload of a bot to a large quantity of vulnerable routers. These exploits don't come cheap, though. The RCE exploit on the router is currently for selling for \$2,500, while and the Telegram 0day is selling for close to \$5,000. If attackers are willing to pay these prices, they can easily skip the line and quickly start creating havoc by building their own large botnet and launching attacks against their intended victims.

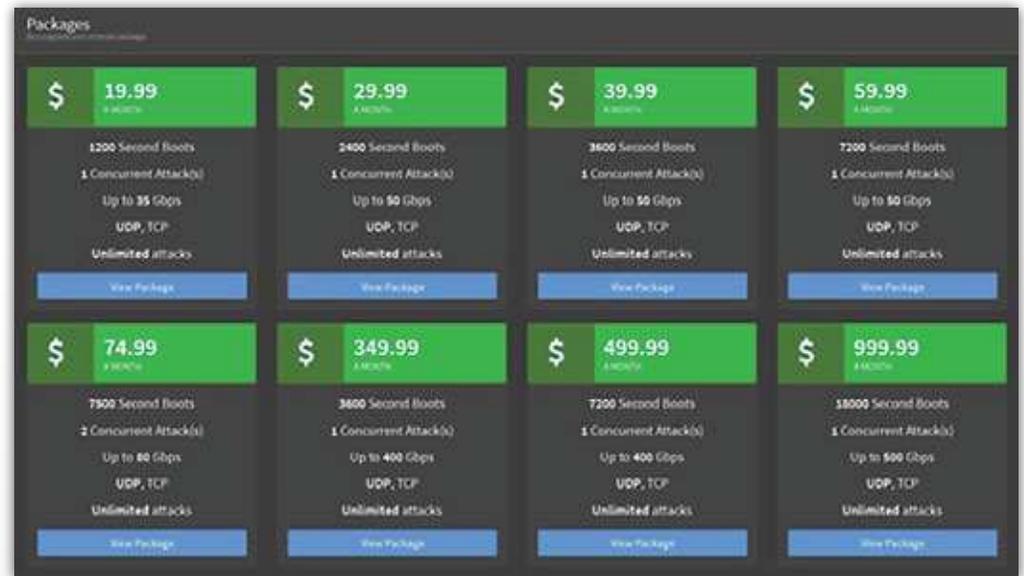


Figure 11. Shenron's DDoS offerings.



Figure 12. RCE over UDP Router Ad.

Off the Shelf at Sellfy

Sellfy is an e-commerce platform that enables members to buy and sell digital content. Its inventory includes a range of benign offerings—with ebooks, comics, design assets, music, video and other digital goods sold by vendors through the Sellfy store front. Vendors can even include a “Buy” button on their own websites.

But dig a little deeper, and it’s easy to find less benign content lurking in the store front. Sellfy also allows vendors to sell malicious digital assets—from attack scripts and services to botnet access and setup. Prices range from just a few dollars to a few hundred.

Any user can simply Google the right keywords and end up at this website. If they come with money in hand, they could leave with a new script—or a complete botnet with over 10,000 bots.

Ransomware

Last but not least: ransomware. It’s among the most popular items for sale in the attack marketplace. Sold in a variety of forms, ransomware ultimately requires the attacker to share some profits with the vendor or operator behind the campaign. For example, Ransom32 is selling on AlphaBay for \$800. Once the attacker purchases the package from the vendor, the attacker specifies how much to ransom the victim for and gives the vendor a Bitcoin address to send payments to. The vendor will then send the purchaser a malicious file that the attacker can send to their victims. The vendor also “graciously” provides attackers with access to a control panel where they can get daily updates about their current campaigns and who has paid.



Figure 13. Ransomware-as-a-service.

The attack marketplace is slowly enabling anyone and everyone to become an attacker if the price is right. For \$19.99 a month, an attacker can run attacks for 30 days, 1,200 seconds at a time utilizing multiple vectors of attack. Those with deeper pockets can shell out \$1,000 and run their own botnet or ransomware campaign.

The bottom line? It doesn’t take much more than an idea and some money to carry out a large-scale attack today. Radware is observing a new breed of attackers who know nothing about hacking other than what site they need to go to—and how much they need to spend to carry out the campaign they envision. Those with more money and less time to invest can immediately start their campaign without the need to learn about anything. The more money you have to spend on attack services, the more you can accomplish without prior experience. These marketplace dynamics are ultimately shifting the scale of the attack landscape.

08

Be Prepared: Key Questions and Actions

Like water, cyber ransom threats tend to take the path of least resistance. When thumbs are stuck in the dike, new holes appear where the foundation is weakest. What follows are key questions to ask—and actions to take—to safeguard your organization.



Key Questions

The key to thwarting cyber-ransom threats: a stronger foundation. Employee education is key in reducing the risk of cyber threats. Now is the time to think through these key questions as they relate to your organization:



How long will it be until we're cyber ransomed?



Are we prepared for cyber ransoms?



Would we ever pay a ransom? If not, why? If so, when?



Who is responsible for making that call?



If cyber ransomed, would we go public? What is our public relations/communications plan?



Do we have internal and external technical resources with the expertise to guide us through these situations?
Do we have privileged access to these resources?



Do we have any insurance to resuscitate any financial losses during the struggle period?



Do we have a legal and/or law enforcement plan in each geography where we operate?



Do we have a policy or plan for cyber hack-back?



Should we consider trial exercises or desktop planning events to help with preparations?



Do we have plans for recovering technical data and infrastructure?

If you have responsibility for any of these areas, don't be a bystander. Be proactive about onboarding controls—and, if your organization affects health and well-being—saving people's lives.

Take Action Today

Cyber ransom is one of a myriad of threats that you now face. Given the complex threat landscape, there are simply no “silver bullet” security solutions. Through our experience helping protect our clients’ critical applications and services, Radware has developed a highly relevant view on what threats pose the greatest risk—and which protection strategies prove most successful.

When it comes to cyber ransom, experience has shown that paying a ransom often leads to prolonged or repeated attacks. A better strategy: turn the economic tables on attackers by making the business a more difficult target through strong security posture. Here’s a checklist for doing just that:



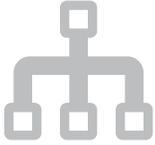
1. Protect Against Availability Attacks

Given the clear and significant correlation between downtime and loss of revenue, avoiding outage resulting from availability attacks should be at the top of the list for any business. With a wealth of sensitive data, it’s not uncommon for organizations to be overly focused on data confidentiality and integrity. This is especially true for those that allow security compliance initiatives to dictate priorities. But with the growth in frequency and severity of DDoS and RDoS attacks, proactive protection is a must.



2. Prepare for Encrypted Attacks

Attacks leveraging encrypted traffic as an attack vector are on the rise, further challenging many of the cyber-threat solutions currently in place. Most cyber-attack mitigation technologies do not actually inspect SSL traffic, as it requires decrypting the encrypted traffic. According to Radware’s 2014-2015 Global Network and Application Security Report, as much as 25% of attack activity today is using SSL-based attack vectors. Organizations should ensure they can address the needs of high capacity mitigation, support all common versions of SSL and TLS, and isolate suspicious encrypted traffic using behavioral analysis to limit legitimate user impact.



3. Protect Assets Behind a CDN

It is increasingly common for businesses to use Content Delivery Networks (CDN) to enhance web application performance. However, CDNs can also be exploited by attackers to launch and even amplify attacks. Dynamic content attacks exploit CDN-based protection by overloading origin servers with requests for non-cached content that the CDN nodes simply pass along. When leveraging CDNs, look carefully at the need for dedicated security protections to sit in front of origin servers.



4. Implement IP-Agnostic Protection

Malicious actors have turned IP address spoofing into an art form. The goal: not only to obfuscate their identity but, in some cases, also to masquerade as seemingly legitimate users based on geo-location or positive reputational information about IP addresses they are able to compromise. Look for solutions that use device fingerprinting technology—employing various tools and methodologies—to gather IP-agnostic information about the source.



5. Consider the CAPEX and OPEX Costs to Processing Unwanted Traffic

Cyber threats continue to grow in size, complexity and duration. Not only do they pose risks associated with data confidentiality, transactional integrity and platform availability, but they also drive up costs associated with processing all of the unwanted data. Processing bad traffic into a data center results in significant costs to any business. Conversely, dropping malicious activity at the perimeter allows an organization to avoid unnecessary operational and capital costs.

In reality, this list could go on and on. It's an all-too-familiar situation for security teams working tirelessly to defend. But the list above provides a solid foundation from which to fight fast-growing and ever-evolving threats—including cyber ransom.

Case study: ProtonMail

In November 2015, the Swiss-based encrypted email provider experienced back-to-back attacks from two different sources—one seeking financial gain and another aiming to undercut ProtonMail’s central mission. Here’s a recap of what happened:

November 3, 2015

Slightly before midnight, ProtonMail received a blackmail email from The Armada Collective, which blackmails companies for Bitcoin under the guise of a DDoS attack. In keeping with The Armada Collective’s standard modus operandi, following this threat was a DDOS attack that took ProtonMail offline for about 15 minutes.

November 4, 2015

11 a.m. – The next DDoS attacks hit ProtonMail’s data center, and its upstream provider begins taking steps to mitigate the attack. However, within a few hours, the attacks take on an unprecedented level of sophistication.

2 p.m. – The attackers directly assault the infrastructure of ProtonMail’s upstream providers and the data center itself. The attack on the company’s ISP exceeded 100Gbps targeting not only the data center, but also routers in Zurich, Frankfurt and other locations where the ISP has nodes. The coordinated assault on key infrastructures successfully brings down both the datacenter and the ISP, affecting not only ProtonMail but also hundreds of other companies.

3:30 p.m. – Under intense third-party pressure, ProtonMail grudgingly pays the ransom to the Bitcoin address 1FxBcZzW3z9NRSUnQ9Pcp58ddYaSuN1T2y. As ProtonMail later noted on its company blog, “This was a collective decision taken by all impacted companies, and while we disagree with it, we nevertheless respected it taking into the consideration the hundreds of thousands of Swiss Francs in damages suffered by other companies caught up in the attack against us. We hoped that by paying, we could spare the other companies impacted by the attack against us, but the attacks continued nevertheless. This was clearly a wrong decision so let us be clear to all future attackers – ProtonMail will NEVER pay another ransom.”

November 5 – 7, 2015

ProtonMail suffers from ongoing, high-volume, complex attacks from a second, unknown source.

November 8, 2015

ProtonMail begins working with Radware’s Emergency Response Team and implements its attack mitigation solution. Service is restored shortly after.

November 9 – 15, 2015

Attacks continue at a high volume, reaching at much as 30Gbps to 50 Gbps at peaks throughout these days. These attacks are successfully mitigated by Radware. At 2:34 p.m. on November 15, a short 2Gbps UDP spike occurs and is blocked. A few minutes later, the attack resumes on UDP. Traffic reaches 7Gbps and is again mitigated. By 11:01, attack volume increases to 17 Gbps, reaching up to 40 Gbps. Again, ProtonMail and Radware continue mitigation. The attack vector then changes, with about 10Gbps hitting infrastructure policy on DP2. Some is matched by DOSS signature DNS reflection, along with ICMP flood; both are successfully mitigated. At 3:20 a.m. on November 16, a short spike of attack, with 150Mbps of traffic coming through was identified and thwarted by Radware.

“We are happy to announce today that after several days of intense work, we have largely mitigated the DDoS attacks against us,” the company reported on its blog on November 10. “These attacks took ProtonMail offline making it impossible to access emails, but did not breach our security. At present, attacks are continuing, but they are no longer capable of knocking ProtonMail offline for extended periods of time. As our infrastructure recovers over the next several days, there may still be intermittent service interruptions, but we have now largely restored all services. Our successful recovery was only possible due to the valiant efforts of IP-Max and Radware, and we would like to sincerely thank them.”

Following the attacks, ProtonMail worked with MELANI, a division of the Swiss federal government, to exchange information with other companies also attacked. It became clear that the attack against ProtonMail occurred in two stages and was arguably two separate campaigns. The first was the volumetric attack targeting only the company’s IP addresses. The second was the more complex attack targeting weak points in the infrastructure of ProtonMail’s ISPs.

As noted on the ProtonMail blog, “This second phase has not been observed in any other recent attacks on Swiss companies and was technically much more sophisticated. This means that ProtonMail is likely under attack by two separate groups, with the second attackers exhibiting capabilities more commonly possessed by state-sponsored actors. It also shows that the second attackers were not afraid of causing massive collateral damage in order to get at us.”

09

Cyber Ransom Lexicon



Bot/Botnet

Group of many (often thousands) of volunteered or compromised computers that send a huge amount of traffic to an attack target, seeking to overwhelm its network.

Clearnet

The term that refers to the traditional World Wide Web. It has relatively low-base anonymity, with most websites routinely identifying users by their IP address. See Darknet.

Clickjacking

Also known as UI redressing, clickjacking is when a user thinks he or she is interacting safely with a legitimate web page, but in fact, there is a malicious script running behind the image or text the user interacts with, aiming to infiltrate his/her computer and steal sensitive data.

Cryptovirus

A form of malware which encrypts data on a user's computer or mobile device, seeking to hold it "hostage" until a ransom payment is made.

Cyber Ransom

A category of information security threat that is growing in scale and sophistication. Its two primary forms are ransomware and ransom denial of service (RDoS) attacks—both of which seek to make digital assets unavailable until a payment is made, typically via a virtual currency.

Darknet

An overlay network that can only be accessed with specific software, configurations or authorization, often using non-standard communications protocols and ports.

Dark Web

Content that exists on Darknet, overlay networks that use the public Internet but which require specific software, configurations or authorization to access.

Deep Web

The parts of the World Wide Web whose contents are not indexed by standard search engines for any reason.

Hijackware

A type of malware that infects an Internet browser in order to display advertising and/or redirect the user to malicious websites. By taking control of a browser's settings, hijackware redirects the user to websites that are written by default into its code. Also known as browser hijacking.

Malicious Software (Malware)

Any type of software that is designed to damage or disable computers and computer systems.

Parasiteware

A type of malware that infects a computer in order to perform various malicious activities. It might display aggressive and unsolicited advertisements and/or redirect affiliate links.

Ransomware

A type of malware that renders a computer or mobile device unusable, typically by encrypting data unless and until a ransom payment is made.

Ransom DDoS

A distributed denial of service (DDoS) attack motivated by monetary gain. Attacks typically start with a letter or post threatening to launch an attack at a certain day and time unless a ransom payment is made. In some cases, attackers will launch a mini-attack on the victim's network as evidence that the threat is real.

Resident Virus

A type of malware that hides and stores itself within the computer's memory. Depending on the virus' programming, it can then infect any file run by the computer. This type of virus even attach itself to anti-virus applications, thereby allowing it to infect any file scanned by the program.

Scareware

A type of malware designed to trick a user into buying and downloading software that is not only unnecessary but also potentially dangerous (fake antivirus protection, for example).

Session Hijacking

Exploitation of a valid computer session to gain unauthorized access to information or services in a computer system. Also known as cookie hijacking.

Trojan Horse

A type of malware which malicious code is contained inside programming or data that appears to be harmless.

Worm

A type of malware that stands alone, replicating itself in order to spread to other computers. Worms may use a computer network to propagate, exploiting security weaknesses in the target computers in order to gain access to them.



For more information, please visit
<http://www.radware.com/Solutions/Security/>

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.

©2016 Radware Ltd. All rights reserved. Radware and all other Radware product and service names are registered trademarks or trademarks of Radware in the U.S. and other countries. All other trademarks and names are property of their respective owners. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications. For more details please see: <https://www.radware.com/LegalNotice/>