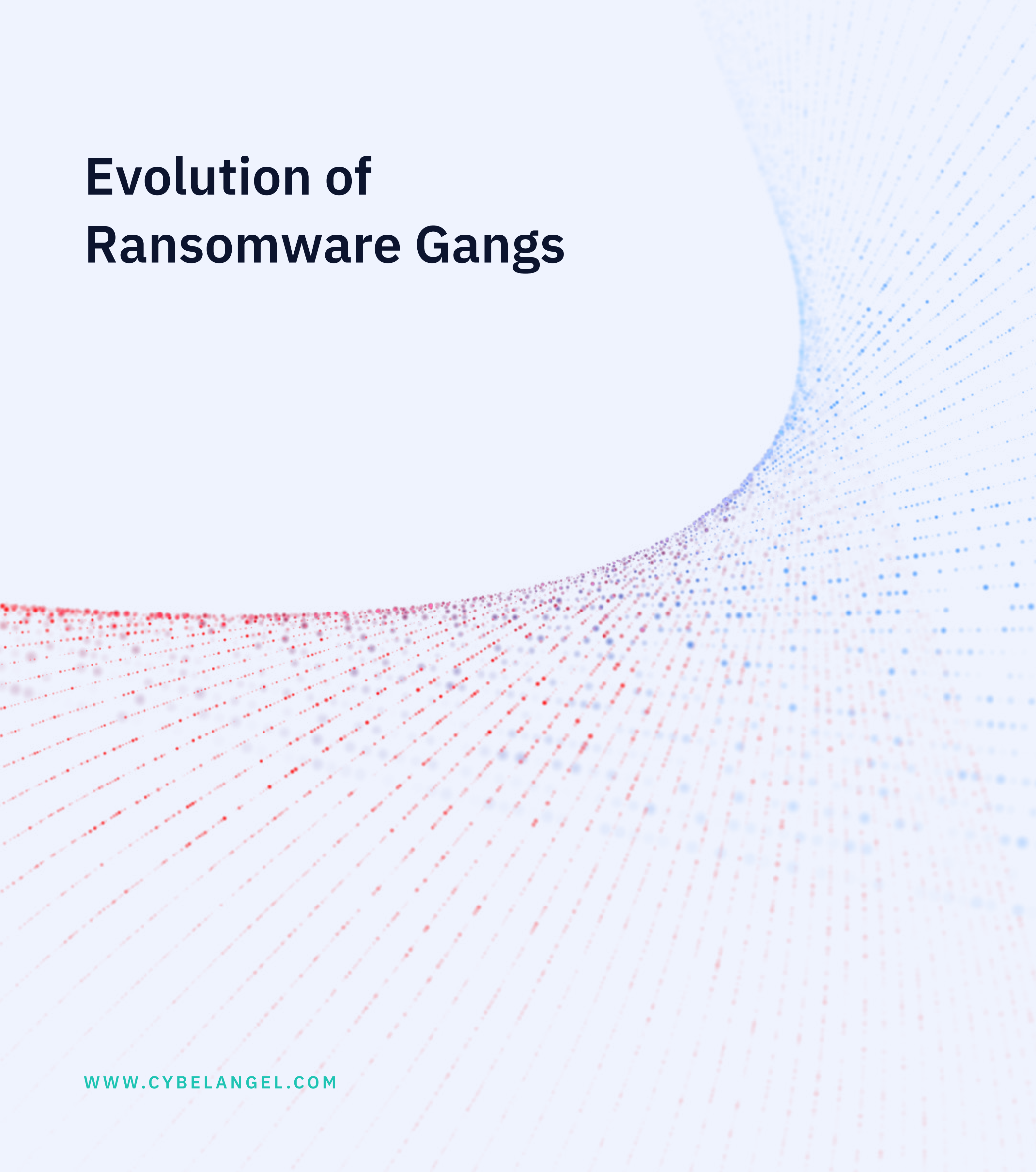
CybelAngel

INDUSTRY ALERT

Evolution of Ransomware Gangs



WWW.CYBELANGEL.COM

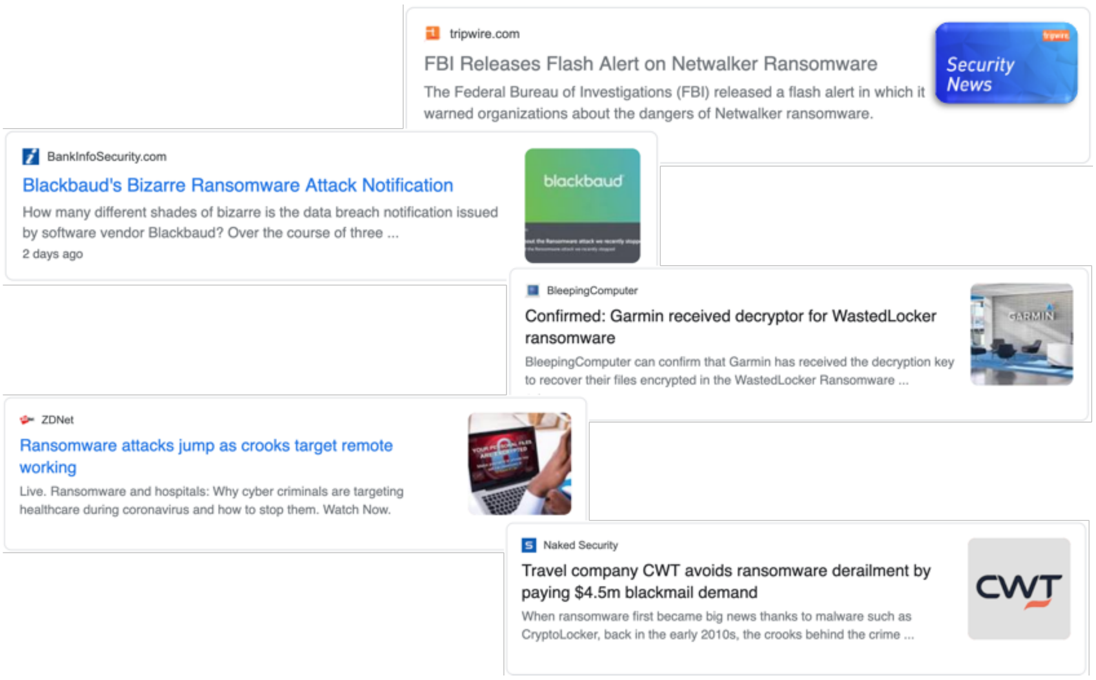
TABLE OF CONTENTS

Evolution of Ransomware Gangs

Introduction

Ransomware is not new, but it still makes front page news by crippling global enterprises and governments. By encrypting all or part of a computer or system, this malware often causes irreparable data loss, even if the owner pays the ransom. Cybersecurity professionals need to stay ahead of the ransomware attacks.

This white paper traces the evolution of ransomware attacks, the different ransomware gangs, and their modus operandi. It helps cyber professionals better understand ransomware from a business and technical perspective, as well as how they can prevent and handle an attack.



tripwire.com

FBI Releases Flash Alert on Netwalker Ransomware

The Federal Bureau of Investigations (FBI) released a flash alert in which it warned organizations about the dangers of Netwalker ransomware.

BankInfoSecurity.com

Blackbaud's Bizarre Ransomware Attack Notification

How many different shades of bizarre is the data breach notification issued by software vendor Blackbaud? Over the course of three ...

2 days ago

BleepingComputer

Confirmed: Garmin received decryptor for WastedLocker ransomware

BleepingComputer can confirm that Garmin has received the decryption key to recover their files encrypted in the WastedLocker Ransomware ...

ZDNet

Ransomware attacks jump as crooks target remote working

Live. Ransomware and hospitals: Why cyber criminals are targeting healthcare during coronavirus and how to stop them. Watch Now.

Naked Security

Travel company CWT avoids ransomware derailment by paying $4.5m blackmail demand

When ransomware first became big news thanks to malware such as CryptoLocker, back in the early 2010s, the crooks behind the crime ...

Ransomware's history

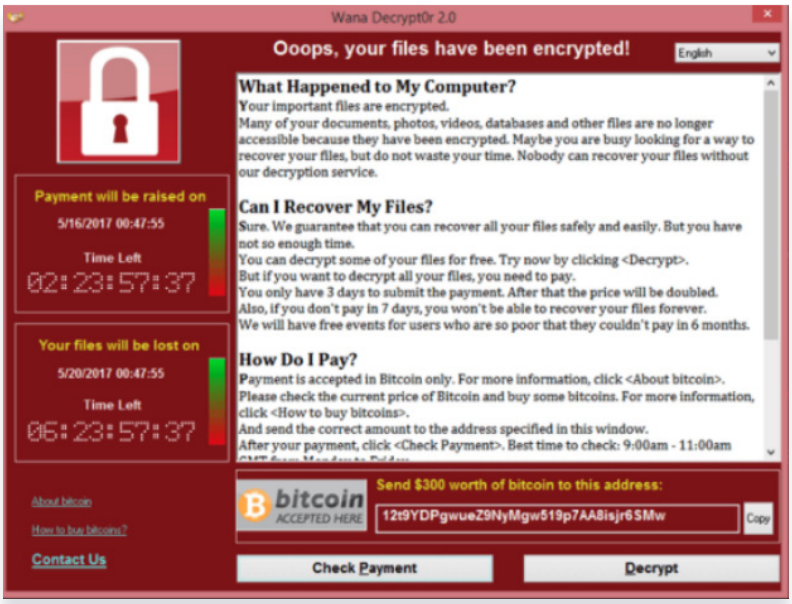
While ransomware has been around for nearly 30 years, the cadence of ransomware attacks is increasingly more effective and more accessible, even to hackers with only a basic technical background.

The first known ransomware attack occurred in 1989 AIDS Trojan[1] which targeted the healthcare industry. While crudely distributed on 20,000 floppy disks, this ransomware attack did manage to infect major corporations, such as Palo Alto Networks.

[1] Becker's Hospital Review. First known ransomware attack in 1989 also targeted healthcare https://www.beckershospitalreview.com/healthcare-information-technology/first-known-ransomware-attack-in-1989-also-targeted-healthcare.html

The next evolution was not until 2012 when the first major global ransomware infection occurred. Reveton Worm or Police Ransomware — so named, as it used a fake FBI (U.S. Federal Bureau of Investigation) message to disguise and lock the computer's data and extort payment from those with infected computers.

Ransomware attacks, as we experience them today, began in 2014 with the first crypto-ransomware with malware, known as Cyrptolocker. This ransomware attack was followed by Petya (2016) and WannaCry (2017), which caused significant economic damage to enterprises across the globe.



What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Evolve or Perish

Like all living things, cybercriminals evolved ransomware by taking a page from legitimate businesses who invested in Software as a Service (SaaS). This next evolution of the malware, Ransomware as a Service (RaaS) is essentially a cloud subscription sold to other hackers.

According to Security Boulevard, "In some cases, there is no subscription fee; many RaaS developers use quasi-affiliate models where the developer collects all of the ransom money extorted by affiliates, takes out some percentage as commission, and passes on the remainder."[2] This malware evolution permits hackers and criminals with very little technical background to lower the barrier to entry and has driven an exponential growth in ransomware attacks.

Ransomware criminals are deploying traditional business processes and techniques. For example, some use advertising schemas on Dark Forums, while others use open auctions to maximize the return on their stolen data or request additional payments to prevent releasing the documents. And still other gangs partner to produce greater results or exploit documents from Victim A to attack Victim B. (See blog for details on recent major attack, Ragnar Locker Targets CWT in Ransomware Attack, July 31, 2020)

[2] Security Boulevard (2019, February 6). What Is Ransomware-as-a-Service? Understanding RaaS. https://security boulevard.com/2019/02/what-is-ransomware-as-a-service-understanding-raas/

Fancy Ransomware Gangs

All flash and sass — this is a fair description of Fancy Ransomware Gangs. These cybercriminals often have cool names, slick logos and websites. Fancy Gangs operate as if they were legitimate businesses using press releases, social media, and service desks in support of their criminal endeavors.

One of the most telling behaviors of Fancy Gangs is exhibited when the victim doesn't pay. In these cases, the group will often publish both a press release on their website and share an excerpt from the stolen documents.

But there can be honor among thieves: If the victim pays the ransom, the criminal enterprise often will not share the pilfered documents; however, this does not mean the data will not be leaked, as was the case with Ragnar Locker. After receiving a reported $4.5M ransom from CWT, Ragnar did share the credentials to the MEGA Cloud Storage with CWT's data. Unfortunately, the credentials were shared on an open chat, which left CWT's 2TB of data exposed until they changed the password. Paying a ransom does not assure an enterprise that their data will not be breached.

Maze is the first Fancy Ransomware Gang to garner wide exposure based on their website beginning in January 2020. By March 2020 (based on domain registrations), quite a few Fancy Gangs had started to publish their own websites, including the DoppelPaymer and Sekhmet gangs. This industrialization of ransomware continues to gain momentum. By July 2020, approximately a dozen actors are known to have published websites where Fancy Ransomware Gangs share extracts of stolen documents to extract ransom fees from their victims.

- AKO (Medusareborn)
- cl0p
- Doppelpaymer
- Maze
- Mespinoza (PYSA)
- Nefilim
- Nemty
- Netwalker
- Ragnar
- REvil (Sodinokibi)
- Sekhmet
- Snatch

(Note: Some of these sites and gangs are no longer active.)

Under the Hood

While ransomware are custom developments, most are forks of other crypto ransomware, which ironically is a bad security habit. REvil, for example, was developed by the actor UNKN and based on GrandCrab. But make no mistake, these codebases are far from identical. In fact, some groups use specific exploit kits and/or CVEs as a unique signature that security researchers can use to identify the origin of the attack. Some examples of ransomware gangs using specific exploit kits and/or CVEs are listed below.

Netwalker
CVE-2019-0708, RDP ("BlueKeep")

Doppelpaymer
CVE-2019-19781, Citrix

Maze
Spelevo & Fallout exploit kits / CVE-2016-7255 / CVE-2018-8453, Windows privilege escalation

REvil
CVE-2018-8453, Windows privilege escalation

These groups also use specific coding techniques, which helps identify the source of a particular attack, including:

- Embedding other tools, such as Cobalt Strike or Mimikatz (French pride \o/), to navigate through infected machine(s) and usually the whole network (SMB, USB port, etc.)
- Developing malware specific to their target (e.g., Netwalkers)
- Using malware armored with anti-VM and anti-RE techniques

Ransomware gangs protect and extend their business operations by maintaining their competitive advantages, such as creating barriers to stop another ransomware from infecting the victim. In addition, they regularly release updated versions with unique new features and conduct competitive espionage to identify opportunities to reverse engineer competitive ransom services.

Modus Operandi

Ransomware behaves similarly to how their gangs operate. Once on the network, the ransomware remains stealth; it sometimes takes up to 300 days before any malicious activity is initiated.

Among the first actions, the ransomware kills critical processes (such as antivirus) and any shadow copies are destroyed. After gaining privileges to the Active Directory (AD), they set a Group Policy Object (GPO) so that all machines get the payload, which may be hidden in the disguise of an image.

Once on the network, the ransomware remains stealth; it sometimes takes up to 300 days before any malicious activity is initiated.

Next, the files targeted in the malware configuration are encrypted one by one. In 76% of these cases, the encryption is done after working hours, using the victim's time zone.[3] Encryption methods vary, with a mix of hard-coded symmetric keys and asymmetric keys. In some cases, different keys may be used for several encrypted servers. Once the encryption is complete, these files are methodically replaced instead of being deleted.

Meanwhile, information about the infected machines is stealthily transmitted back to the ransomware group. Data may be exfiltrated in 7z archives through FTP with credentials hardcoded within the malware. The gangs determine the ransom amount based on the elements found. According to the Beazley Group, the current ransom is pegged at $13,000, while the highest confirmed ransom paid — at the time of this writing — is $930,000.[4]

So, you've been infected

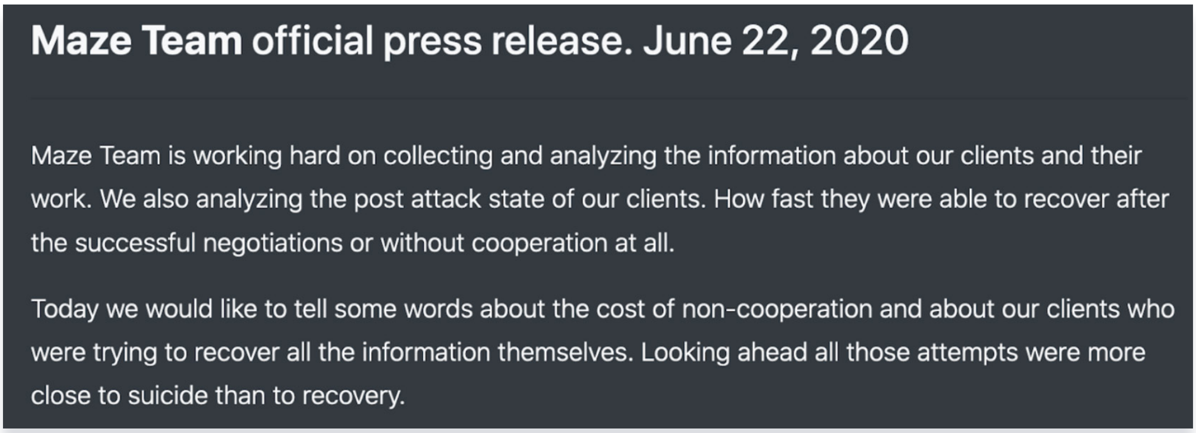
The ransom note arrives. It includes an identifier, which consists of your company name, plus a key. You are instructed to send your identifier to the Ransomware Gang on their website, along with the ransom in bitcoin. If you pay the ransom, the group will retrieve the victim's private key thanks to cryptographic operations.

What do you do? Pay or don't pay? Will you get your data back or not?

Paying the ransom may seem like a good option, but as previously discussed it does not guarantee your enterprise will not be the victim of a data breach.

If your network is infected by a Fancy Gang, it is likely that no one knows about the attack except you and the ransomware gang. When you pay, the gang will send you credentials to access your data returned. Som companies with cyber insurance may even be reimbursed for their damages. However, there is a high likelihood your data may have been leaked, and a major data breach is around the corner.

Aggressive ransomware gangs take a different approach to increase the chances of receiving a large ransom. Many publicly threaten to shame victims and their companies into paying the ransom. The ways these gangs shame their victims ranges from Maze's "press releases," which detail the failure of negotiations and in many cases expose the names of executives and employees. Whereas *Ragnar* uses a "wall of shame," other gangs, such as *Nefilim*, shame victims on their homepage, where they employ a live countdown until the stolen documents are published.


Maze Team official press release. June 22, 2020

Maze Team is working hard on collecting and analyzing the information about our clients and their work. We also analyzing the post attack state of our clients. How fast they were able to recover after the successful negotiations or without cooperation at all.

Today we would like to tell some words about the cost of non-cooperation and about our clients who were trying to recover all the information themselves. Looking ahead all those attempts were more close to suicide than to recovery.

[3] Fireeye (2020, March 16). They Come in the Night: Ransomware Deployment Trends. https://www.fireeye.com/blog/threat-research/2020/03/they-come-in-the-night-ransomware-deployment-trends.html

[4] Comparitech (2020, June 15). 2018-2020 Ransomware Statistics and Facts. https://www.comparitech.com/antivirus/ransomware-statistics/

Not paying the ransom comes at an equally high price. As Baltimore City demonstrated in 2019, the ransom is often significantly less than the cost to recover from the ransomware attack. It is estimated that Baltimore's recovery was a staggering $18 million dollars — crippling the government for over a month and impacting vaccine production, ATMs, airports, and hospitals — whereas, the ransom was only $76,000 in bitcoin. This is far from an isolated case. We only need to look one year earlier to find that in 2018, it cost the city of Atlanta $17 million dollars to recover after a ransomware attack.[5]

> "… it cost the city of Atlanta $17 million dollars to recover after a ransomware attack."[5]

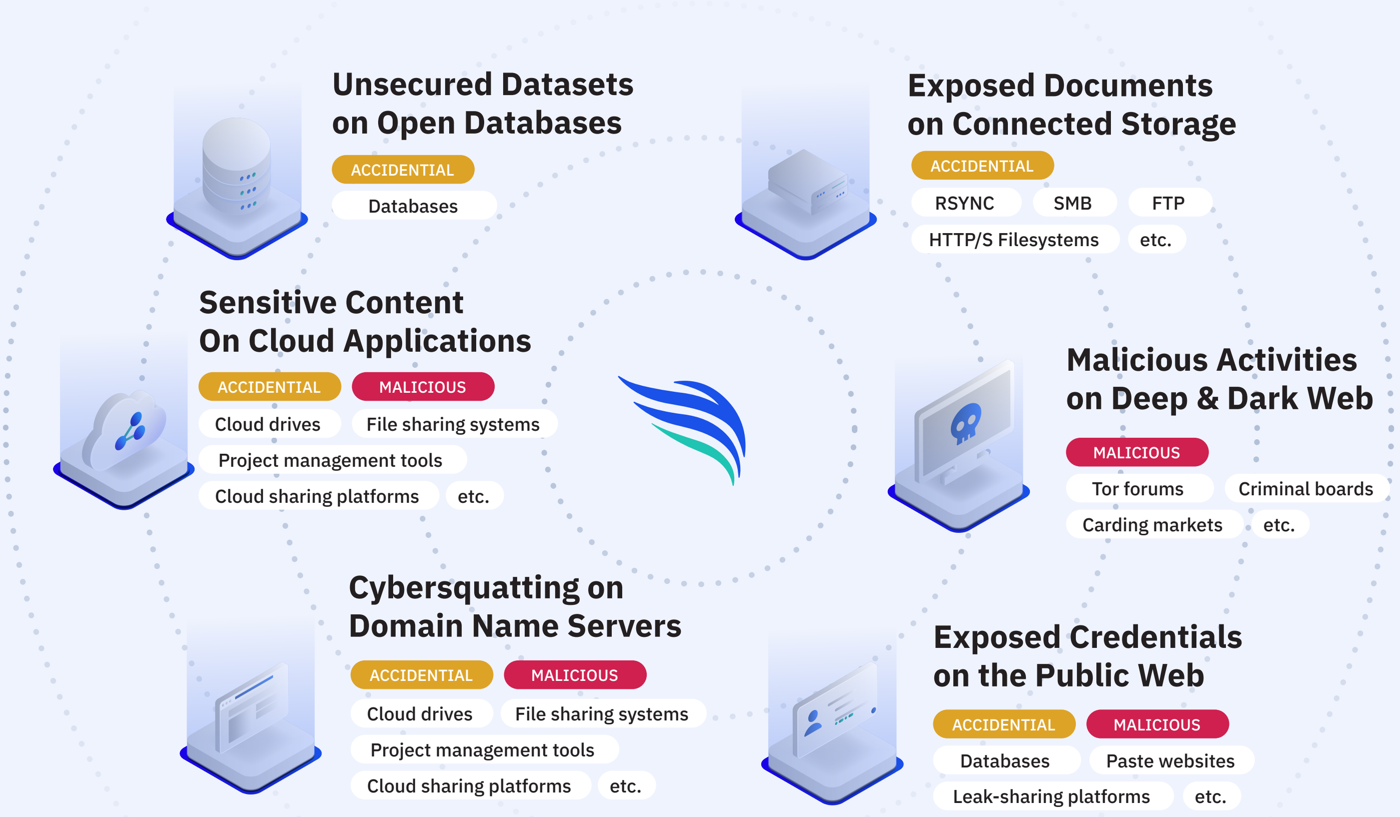
CybelAngel's digital risk protection

Cybercriminals don't advertise the names of corporations they plan to attack; and once the corporation is targeted, it is often too late to prevent harm. What is even more worrisome is these ransomware attacks have occurred on a massive scale, using critical CVE that IT departments have not found time to deploy.

One of the best steps you can take to protect your digital assets is to take charge of your digital footprint with digital risk protection solutions.

Using CybelAngel's platform, you can detect leaks and vulnerabilities — yours, your supply chain, and your third party's. Taking actions to thwart the hackers and cyber criminals before they wreak havoc on your enterprise.

CybelAngel's digital risk protection and data safeguarding is comprehensive.



Unsecured Datasets on Open Databases

ACCIDENTIAL

Databases

Exposed Documents on Connected Storage

ACCIDENTIAL

RSYNC | SMB | FTP | HTTP/S Filesystems | etc.

Sensitive Content On Cloud Applications

ACCIDENTIAL | MALICIOUS

Cloud drives | File sharing systems | Project management tools | Cloud sharing platforms | etc.

Malicious Activities on Deep & Dark Web

MALICIOUS

Tor forums | Criminal boards | Carding markets | etc.

Cybersquatting on Domain Name Servers

ACCIDENTIAL | MALICIOUS

Cloud drives | File sharing systems | Project management tools | Cloud sharing platforms | etc.

Exposed Credentials on the Public Web

ACCIDENTIAL | MALICIOUS

Databases | Paste websites | Leak-sharing platforms | etc.

[5] IBID

- Connected Storage - Locate and safeguard confidential documents negligently made available on corporate and third-parties' connected storage.
- Cloud Applications - Identify and troubleshoot sensitive content leaking through collaborative tools, repositories and cloud applications used by your company or third parties.
- Open Databases - Detect and secure misconfigured databases before they are compromised.
- Domain Name Servers - Prevent phishing, counterfeiting and domain squatting attempts before your business is harmed.
- Public Web - Secure exposed sensitive credentials before they are weaponized.
- Deep and Dark Web - Intercept and defend against threat campaigns or fraud schemes on malicious forums before hostile attacks are launched.

Learn how CybelAngel can protect your company. CONTACT US NOW.

About CybelAngel

CybelAngel reduces global enterprise digital risk by detecting critical data leaks outside the firewall before these leaks become major data breaches. Leveraging its Augmented Intelligence, a unique combination of proven machine learning capabilities and superior cyber analysts, CybelAngel analyzes billions of data sources, thousands of files, and hundreds of threats across all layers of the internet to discover critical data leaks for their customers. Global organizations rely on CybelAngel every day to detect critical data leaks before wreaking havoc on their business.

Learn more at www.cybelangel.com

PARIS | NEW YORK | LONDON