

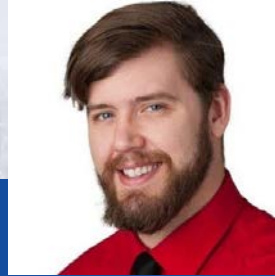


Cybercrime Tactics & Techniques: Q2 2019

Ransomware Retrospective

Jarryd Boyd, Senior Engineer

Who Am I?



Jarryd Boyd, Senior Sales Engineer

Years of experience fighting cyber threats, from the networks to the endpoint.

Deep seeded belief in multi layered security approaches

Has worked with fortune 500 companies and small businesses

Key Takeaways

» Ransomware shifts to business targets

- » Consumer ransomware drops -12% YoY & -25% QoQ
- » Business focused ransomware increase by 365% YoY
- » Ryuk ransomware increase 88% QoQ
- » GandCrab ransomware decreased 33% QoQ
- » Ransomware against businesses is a better return on investment (ROI)
- » Ransomware evolution will continue, making it more difficult to defend against



RANSOMWARE

AIMS HIGHER



Why the shift?

Business attacks have surged in 2019

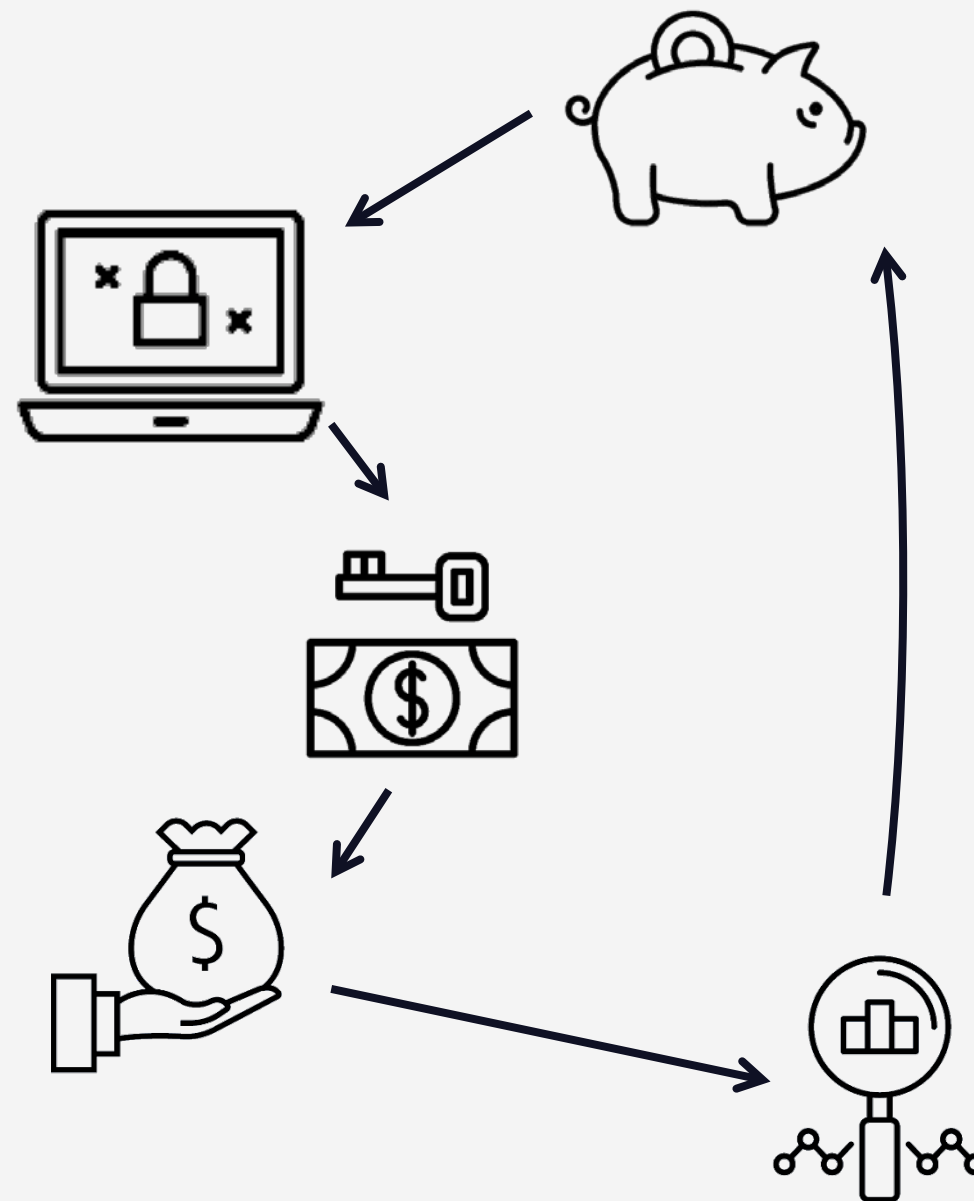
- » *At least double the amount of public attacks in 2018*
- » *Municipal networks have been identified as easy and valuable targets*
- » *Schools, healthcare facilities and manufacturing firms also big targets for these threats*



Why the shift?

Return on Investment

- » *More Valuable Targets*
- » *Greater Ransom*
- » *Easier to spread*
- » *Payment is more likely*



Why the shift?

New Technologies

- » *EternalBlue*
- » *WannaCry & NotPetya*
- » *Trickbot & Emotet*



DETECTIONS



Consumer Product Ransomware Detections 2018 – 2019

Consumer Products

Ransomware Family	YoY % Change 2018-2019	QoQ % Change Q1 - Q2
All Ransomware	-12%	-25%
GandCrab	-54%	-40%
Ryuk	NEW	-55%
Troldesh	162%	-45%
Rapid	-30%	-57%
Locky	-54%	-24%

Business Product Ransomware Detections 2018 – 2019

Business Products

Ransomware Family

YoY % Change 2018-2019

QoQ % Change Q1 - Q2

All Ransomware

363%

14%

GandCrab

NEW

88%

Ryuk

24%

-5%

Troldesh

NEW

-47%

Rapid

NEW

940%

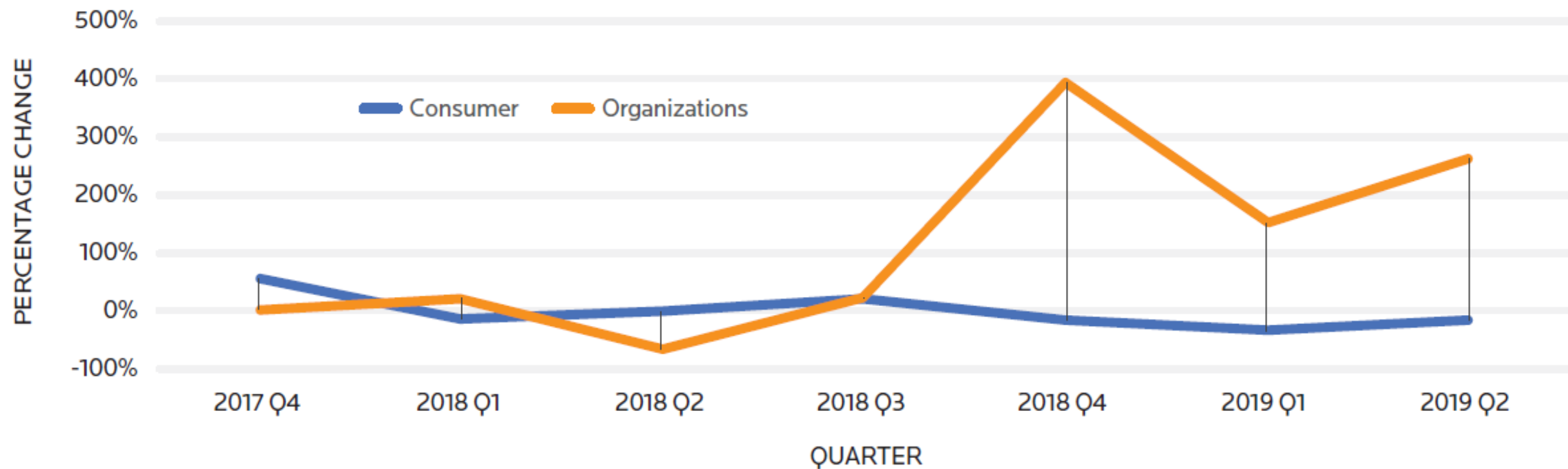
Locky

319%

19%

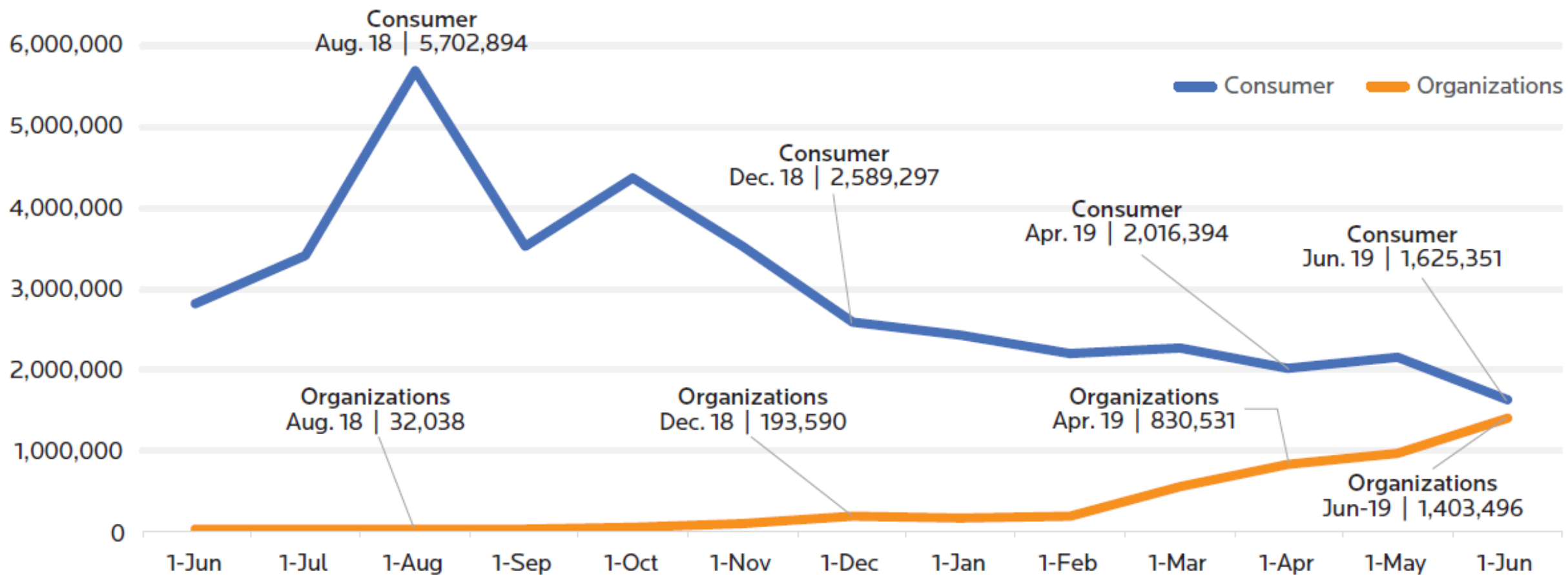
	2017 Q4	2018 Q1	2018 Q2	2018 Q3	2018 Q4	2019 Q1	2019 Q2
Consumer	55%	-13%	-1%	22%	-16%	-34%	-16%
Business	2%	22%	-66%	23%	393%	152%	263%

Ransomware Detections Percentage Comparison by Quarter Q4 2017 - Q2 2019



Ransomware shifts from consumer to business

Ransomware Target Focus 12 Month View | Jun. 18 - June 19

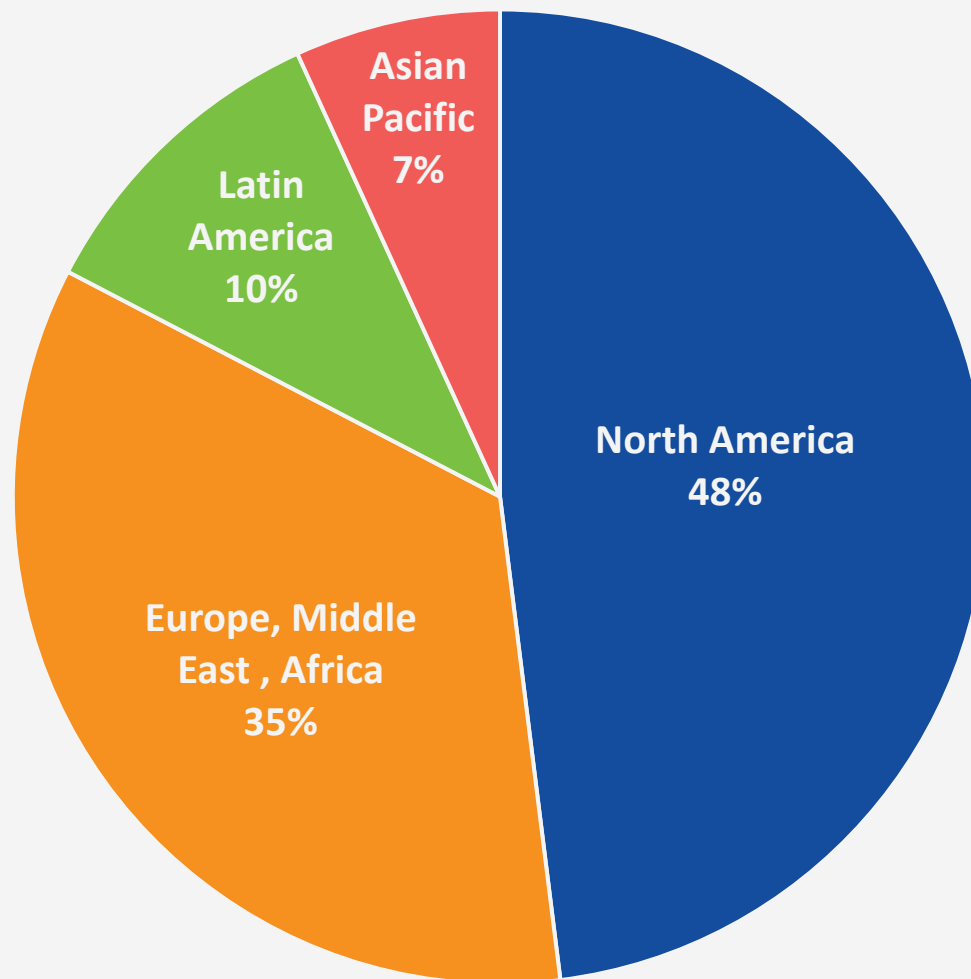


REGIONAL BREAKDOWN



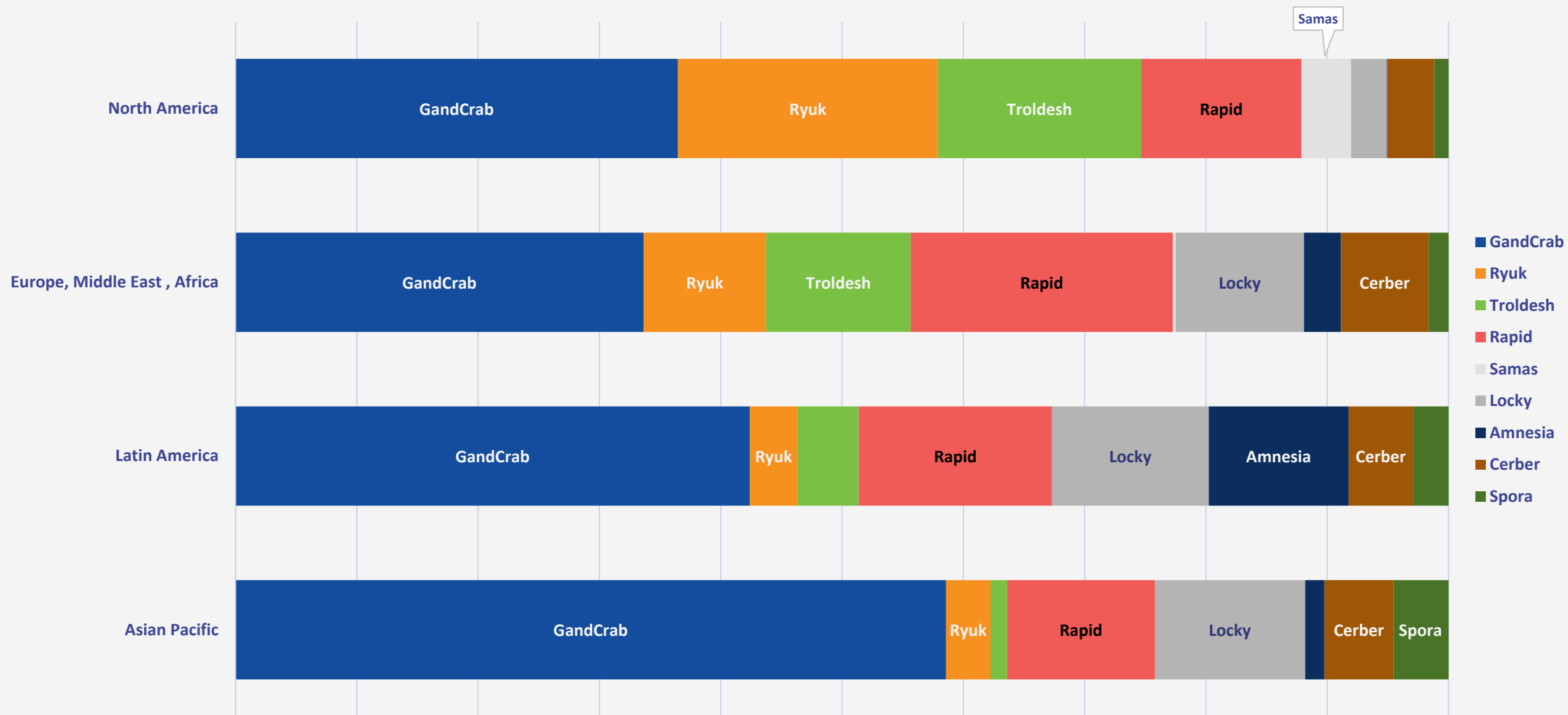
Region Breakdown by Ransomware Detection Jun 2018 - Jun 2019

Business + Consumer Products



Top 5 Ransomware Family by Region Jun 2018 - Jun 2019

Business + Consumer Products

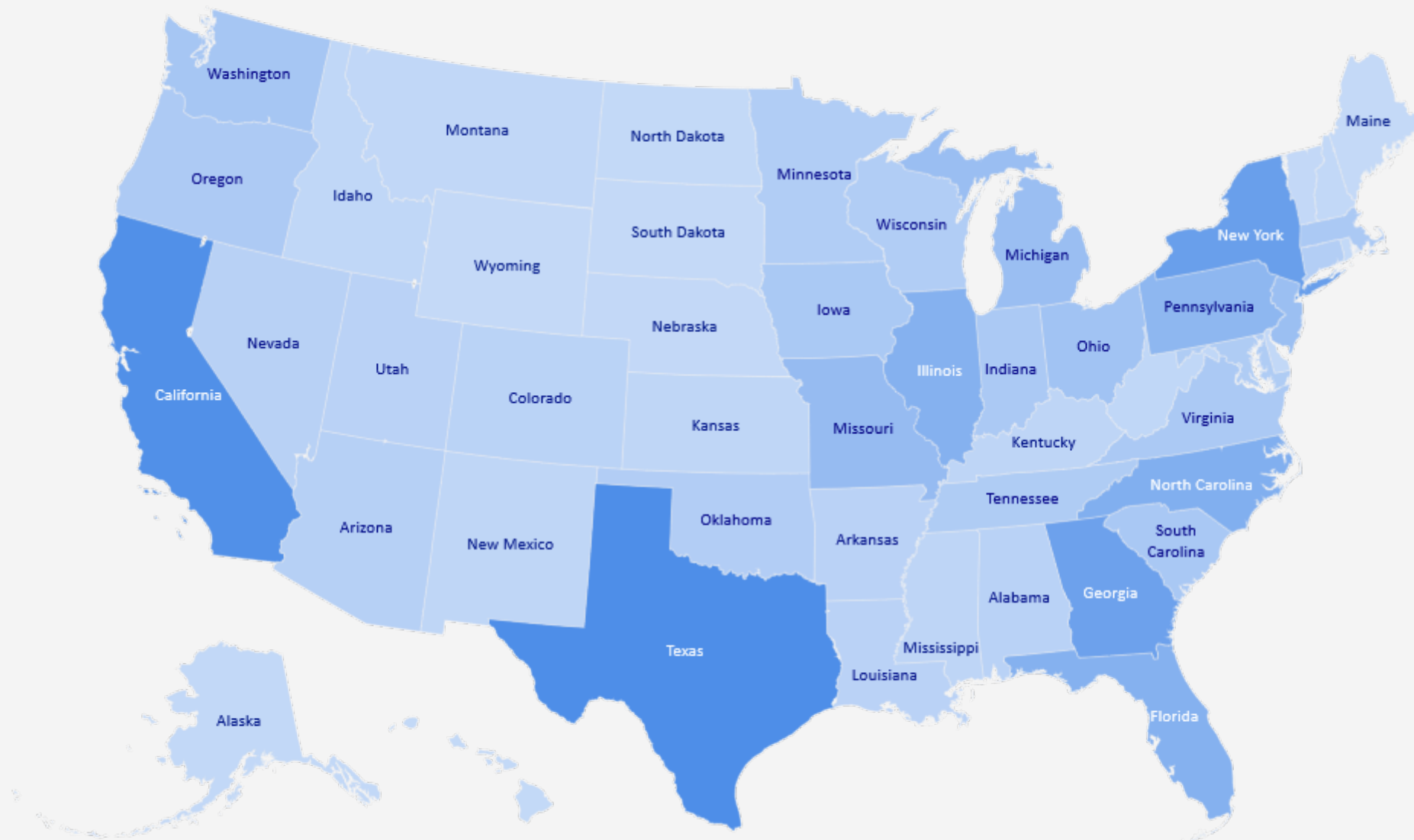


United States Ransomware Detection Jun 2018 - Jun 2019
Business & Consumer Products

United States

States Most Effectuated:

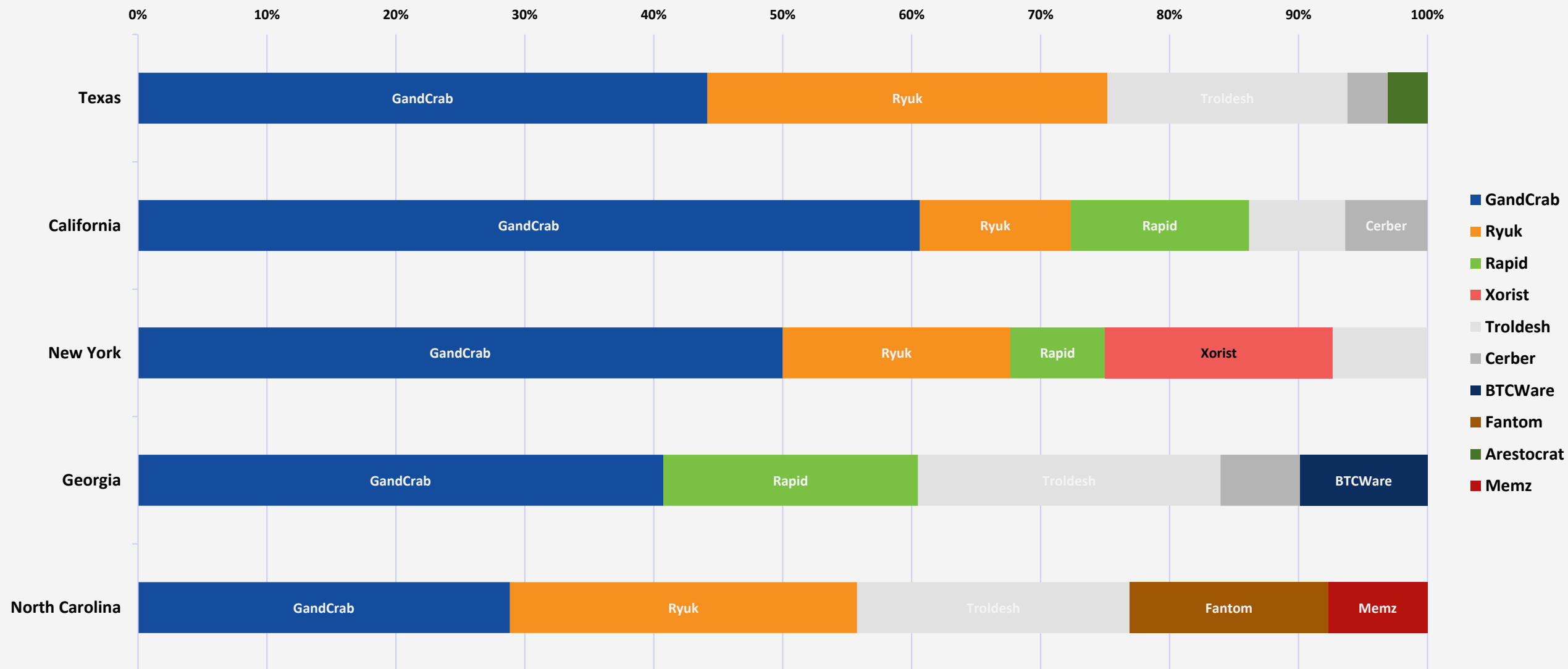
- » *Texas*
- » *California*
- » *New York*
- » *Georgia*
- » *North Carolina*



Top 5 Ransomware Family Detections by Top 5 U.S. States

Jun 2018 - Jun 2019

Business & Consumer Products



RANSOMWARE FAMILIES



GandCrab Ransomware

» GandCrab Facts

- » Ransomware as a Service
- » Multiple Evolutions
- » Authors claim to have retired
- » Methods of infection
 - » Exploits
 - » Emails

We are sorry, but your files have been encrypted!

Don't worry, you can return all your files! We can help you!

Files decryptor price is **400 USD**

If payment is not made before **2018-03-17 06:04:51 UTC** the cost of decrypting files will be doubled

Time left to double price:

01 days 23h:59m:06s

What happened?
Your computer have been infected with GandCrab Ransomware. Your files have been encrypted and you can't decrypt it yourself.

In the network, you can find [decryptors](#) and third-party software, but it will not help you and **can make your files undecryptable**.

What can I do to get back my files?
You should buy **GandCrab Decryptor**. This software will decrypt all your encrypted files and remove GandCrab Ransomware from your PC. Current price: **\$400.00**. For payment you need cryptocurrency **DASH**

What guarantees can you give me?
You can use test decryption and decrypt 1 file for free.

What is DASH and how can I purchase GandCrab Decryptor?
You have a few ways to buy **DASH**. Abbreviation - **DSH**.


Exchange listing	dash.org
CEX.IO	<ul style="list-style-type: none"> • Credit/Debit card • Bank transfer • CryptoCapital
alfacashier.com	<ul style="list-style-type: none"> • Perfect Money • Money Polo • ChinaUnionPay CNY • Thailand Banks THB
24xbtc.com	<ul style="list-style-type: none"> • Western Union

[Buy GandCrab Decryptor](#) Support 24/7 Test Decrypt

DASH 1 DSH = \$392.10

Payment amount **1.02014792 DSH**

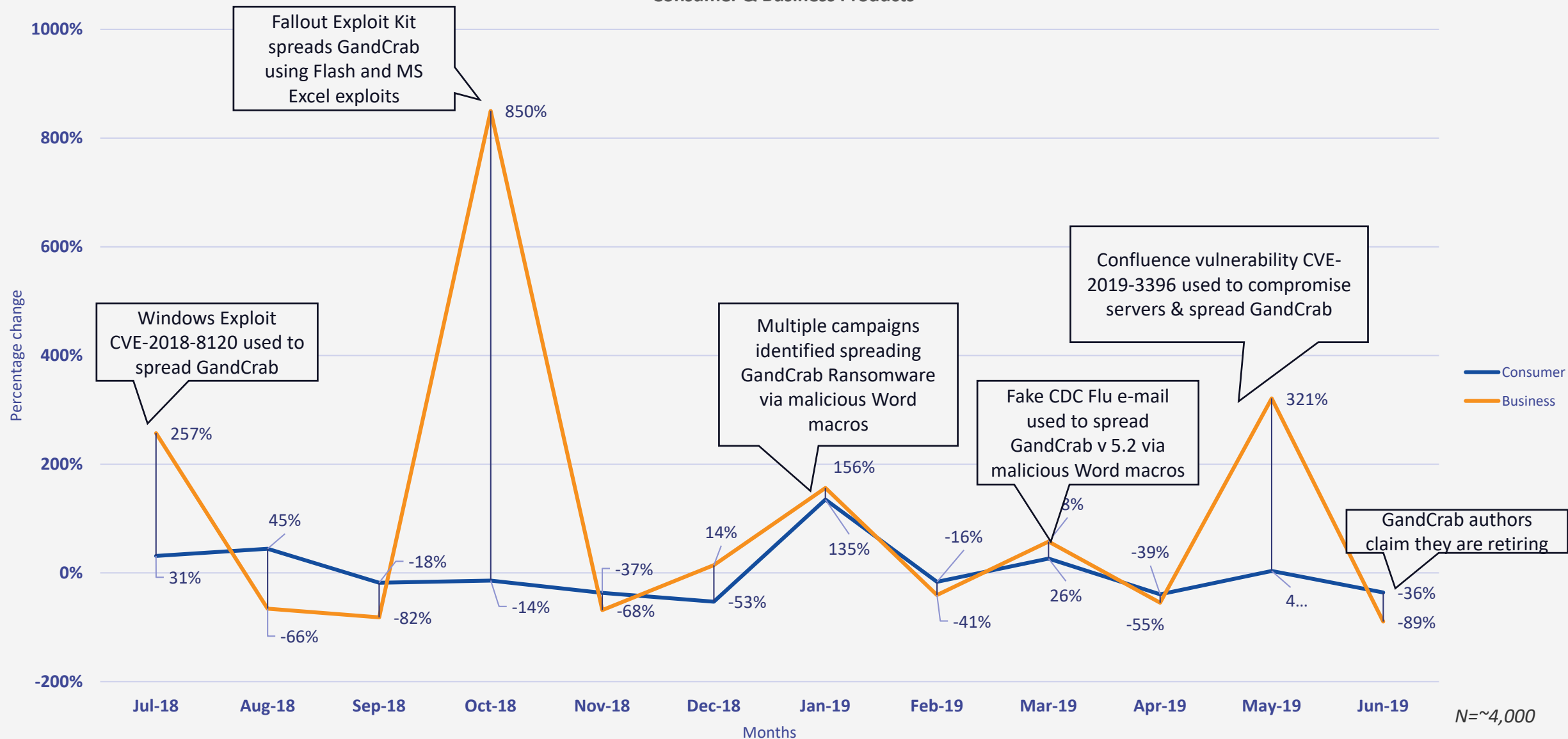
To complete a payment, please send
1.02014792 DSH
 to the address
XpwA2qET7GA4jaS3kNpS6xPqjSxXZNbEQN
 (~ \$400.00)



TXID	Amount	Status
None.		

GandCrab Detections by Percentage Changes Jun 18 - Jun 19

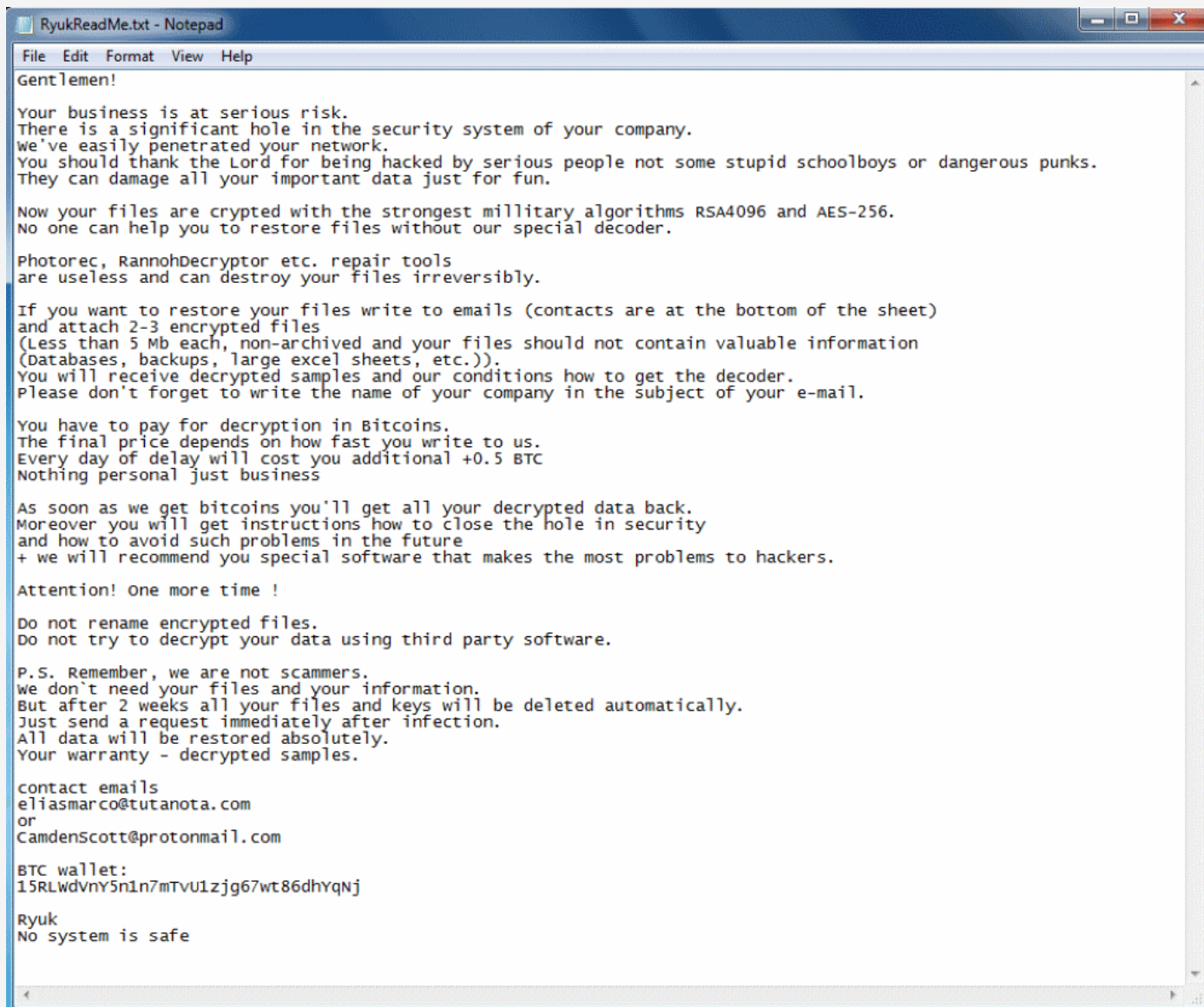
Consumer & Business Products



Ryuk Ransomware

» Ryuk Facts

- » First observed in mid 2018
- » Most commonly seen business ransomware in 2019
- » Part of the “Triple Threat”
- » Derived from the “Hermes” ransomware
- » Utilizes RSA 2048 & AES 256 encryption



```
RyukReadMe.txt - Notepad
File Edit Format View Help
Gentlemen!

Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous punks.
They can damage all your important data just for fun.

Now your files are crypted with the strongest millitary algorithms RSA4096 and AES-256.
No one can help you to restore files without our special decoder.

Photorec, RannohDecryptor etc. repair tools
are useless and can destroy your files irreversibly.

If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.
Please don't forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
Every day of delay will cost you additional +0.5 BTC
Nothing personal just business

As soon as we get bitcoins you'll get all your decrypted data back.
Moreover you will get instructions how to close the hole in security
and how to avoid such problems in the future
+ we will recommend you special software that makes the most problems to hackers.

Attention! One more time !

Do not rename encrypted files.
Do not try to decrypt your data using third party software.

P.S. Remember, we are not scammers.
We don't need your files and your information.
But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty - decrypted samples.

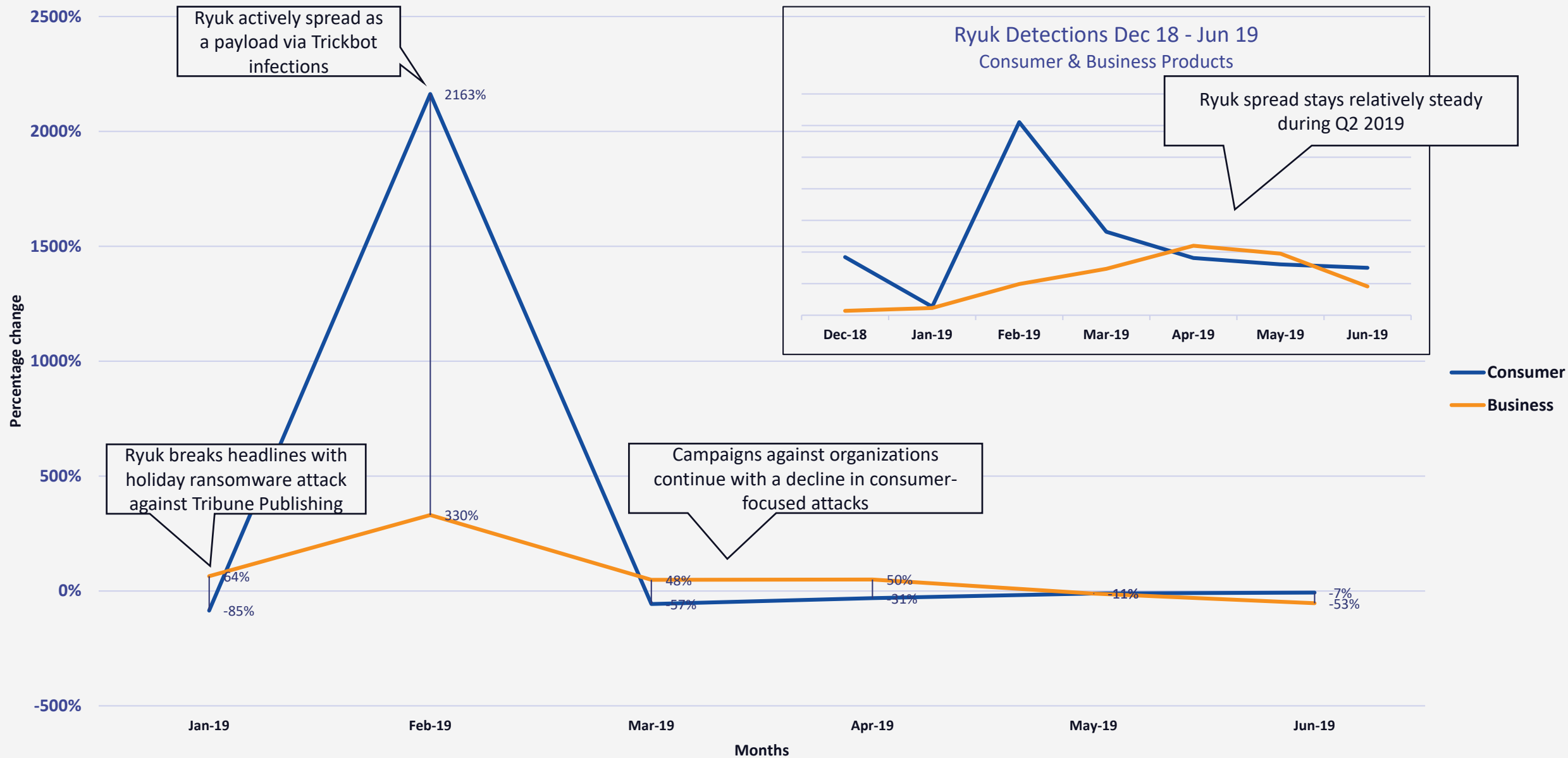
contact emails
eliasmarco@tutanota.com
or
CamdenScott@protonmail.com

BTC wallet:
15RLWdVnY5n1n7mTVU1zjg67wt86dhvQnJ

Ryuk
No system is safe
```

Ryuk Detections by Percentage Changes 2019

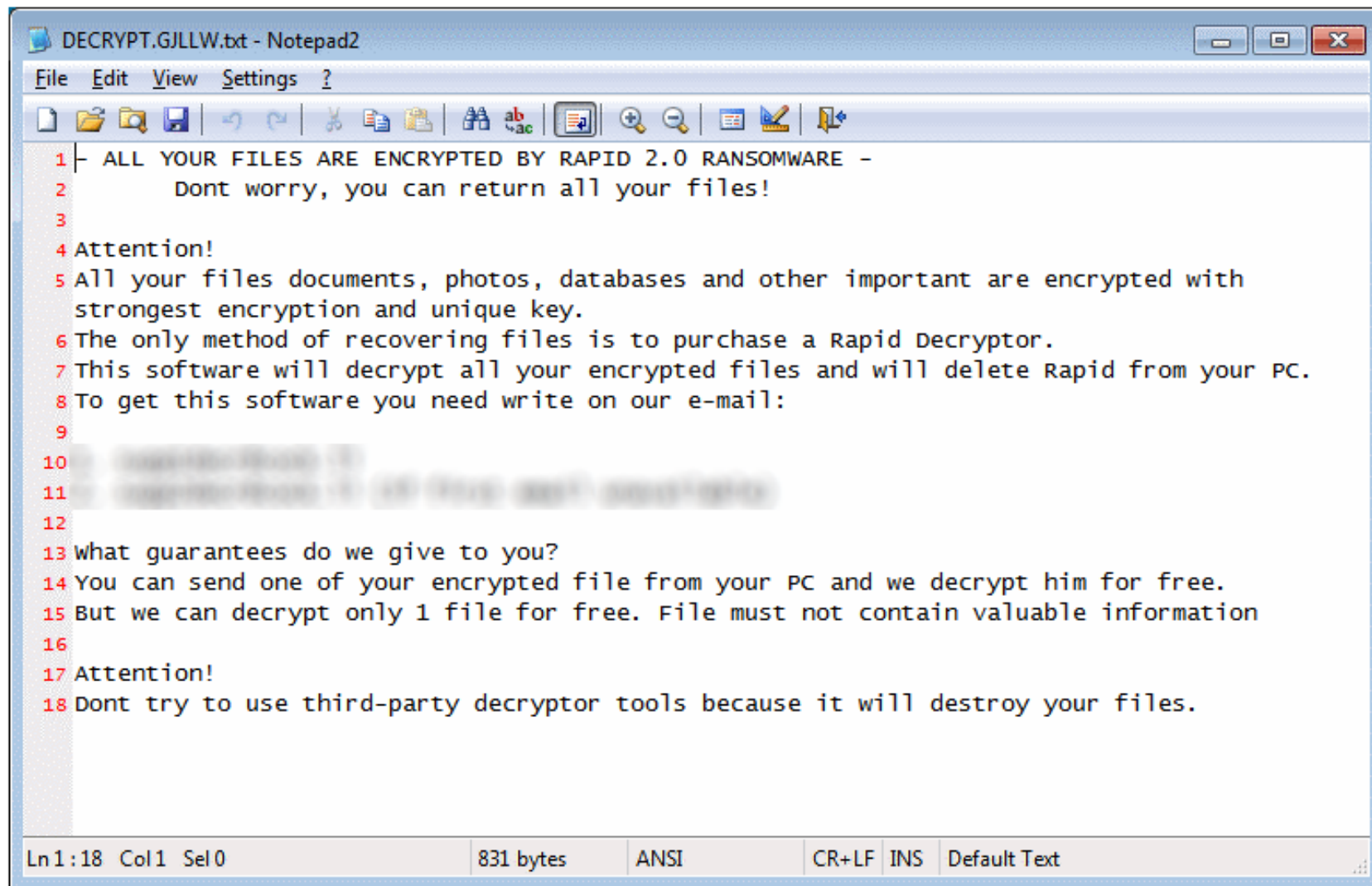
Consumer & Business Products



Rapid Ransomware

» Rapid Facts

- » First discovered in 2017
- » Spread through
 - » Malicious e-mails
 - » Manual Infection
- » Rapid infections went up 200% between May and June 2019



DECRYPT.GJLLW.txt - Notepad2

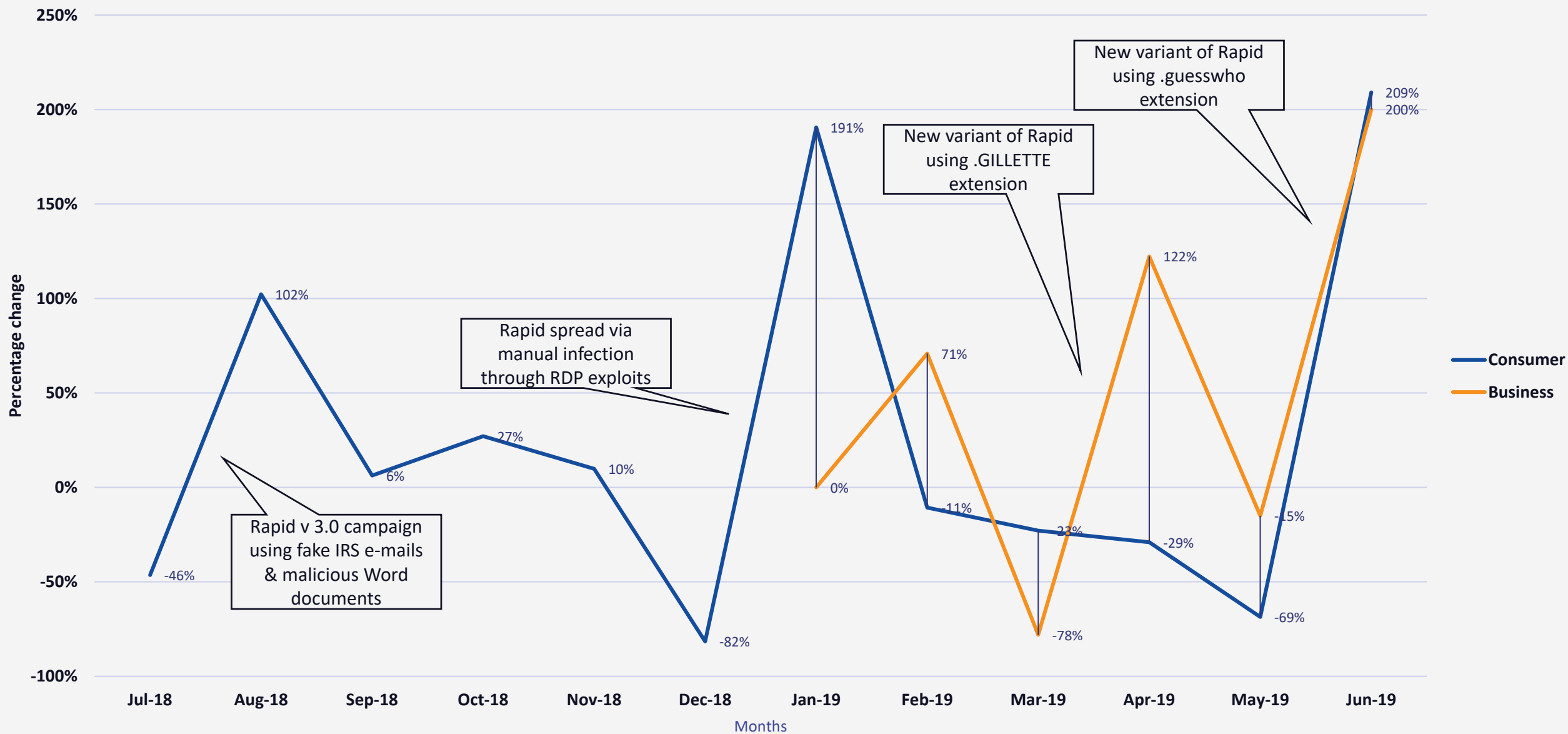
File Edit View Settings ?

1 | ALL YOUR FILES ARE ENCRYPTED BY RAPID 2.0 RANSOMWARE -
2 | Dont worry, you can return all your files!
3 |
4 | Attention!
5 | All your files documents, photos, databases and other important are encrypted with
6 | strongest encryption and unique key.
7 | The only method of recovering files is to purchase a Rapid Decryptor.
8 | This software will decrypt all your encrypted files and will delete Rapid from your PC.
9 | To get this software you need write on our e-mail:
10 | [REDACTED]
11 | [REDACTED]
12 |
13 | what guarantees do we give to you?
14 | You can send one of your encrypted file from your PC and we decrypt him for free.
15 | But we can decrypt only 1 file for free. File must not contain valuable information
16 |
17 | Attention!
18 | Dont try to use third-party decryptor tools because it will destroy your files.

Ln1:18 Col1 Sel0 831 bytes ANSI CR+LF INS Default Text

Rapid Ransomware Detections by Percentage Changes Jun 18 - Jun 19

Consumer & Business Products



Troldesh Ransomware

» Troldesh Facts

- » Also Known As “Shade”
- » Been around for many years
- » Spread through malicious e-mail.
- » Utilized compromised CMS platforms to host malware
- » Historically focused on Russia until 2018.



ВНИМАНИЕ!

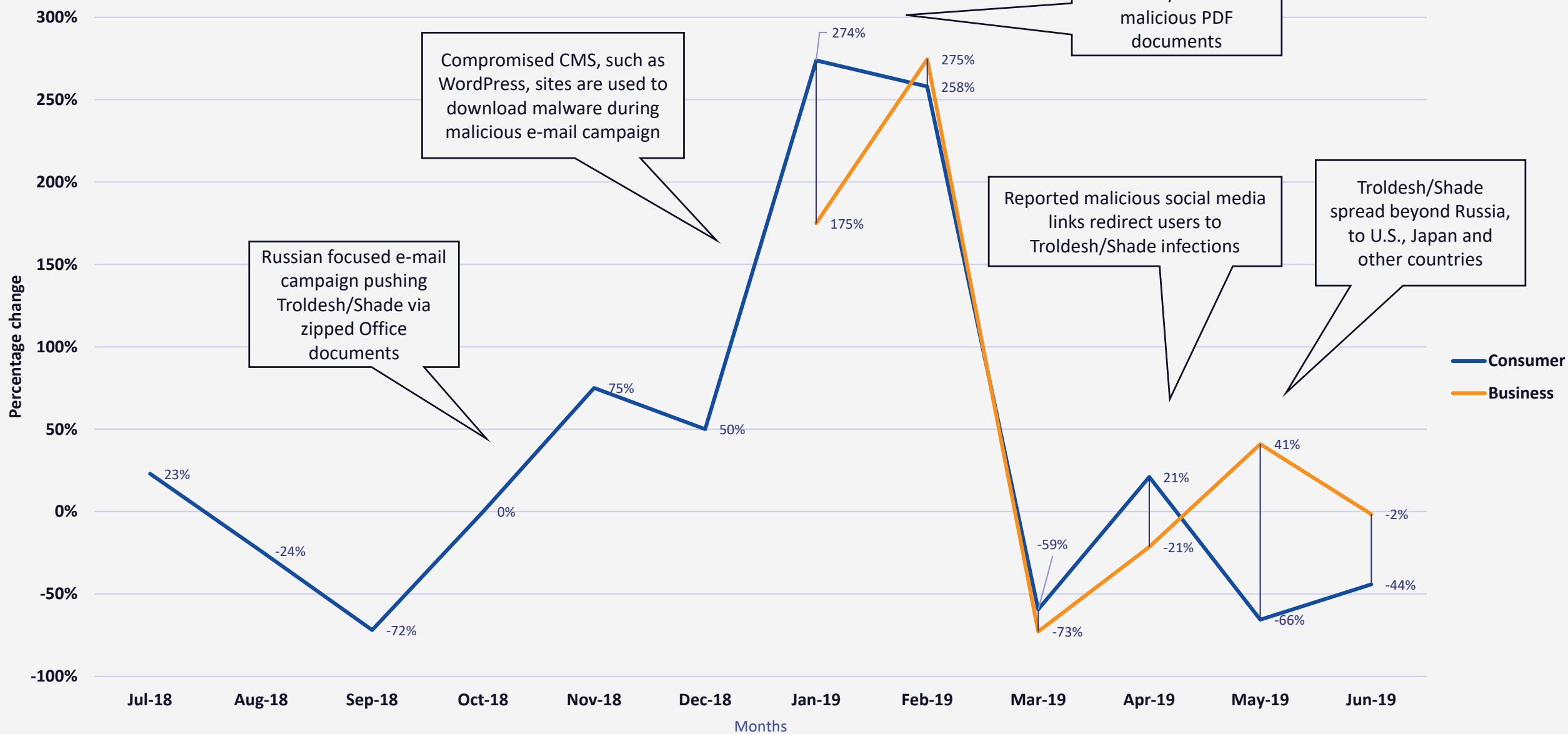
Все важные файлы на всех дисках вашего компьютера были зашифрованы.

Подробности вы можете прочитать в файлах README.txt, которые можно найти на любом из дисков.

ATTENTION!

**All the important files on your disks were encrypted.
The details can be found in README.txt files which you can find on any of your disks.**

Troldesh Detections by Percentage Changes Jun 18 - Consumer & Business Products



Locky Ransomware

» Locky Facts

- » Offline since 2018
- » First appeared in 2016
- » Upgraded multiple times
- » Functionality to hide malware & better encryption

```
_*+-$||-*  
$_-|~__$~*_+$_-
```

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.

More information about the RSA and AES can be found here:

[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:

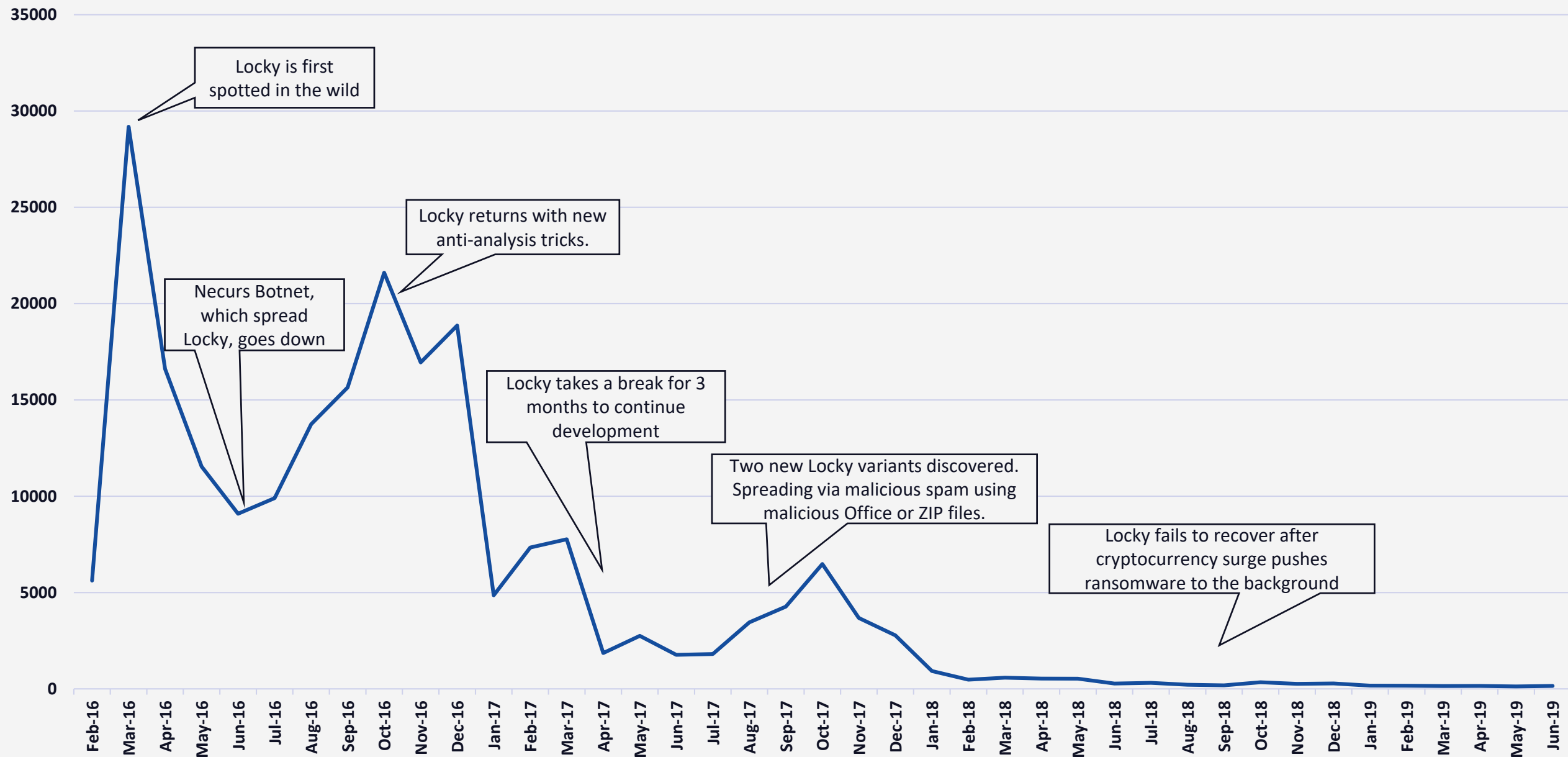
If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: <https://www.torproject.org/download/download-easy.html>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: g46mbrrzpfszonuk.onion/
4. Follow the instructions on the site.

!!! Your personal identification ID: [REDACTED] !!!

```
+==*~|
```

Locky Detections Feb 16 - Jun 19



Cerber Ransomware

» Cerber Facts

- » First discovered March 2016
- » First Ransomware as a service
- » Most commonly seen ransomware of 2016
- » Dec 2017, five Romanian nationals were arrested.
- » Cerber went down shortly after that.

Your documents, photos, databases and other important files have been encrypted by "Cerber Ransomware 4.1.5"!

If you understand all importance of the situation then we propose to you to go directly to your personal page where you will receive the complete instructions and guarantees to restore your files.

There is a list of temporary addresses to go on your personal page below:

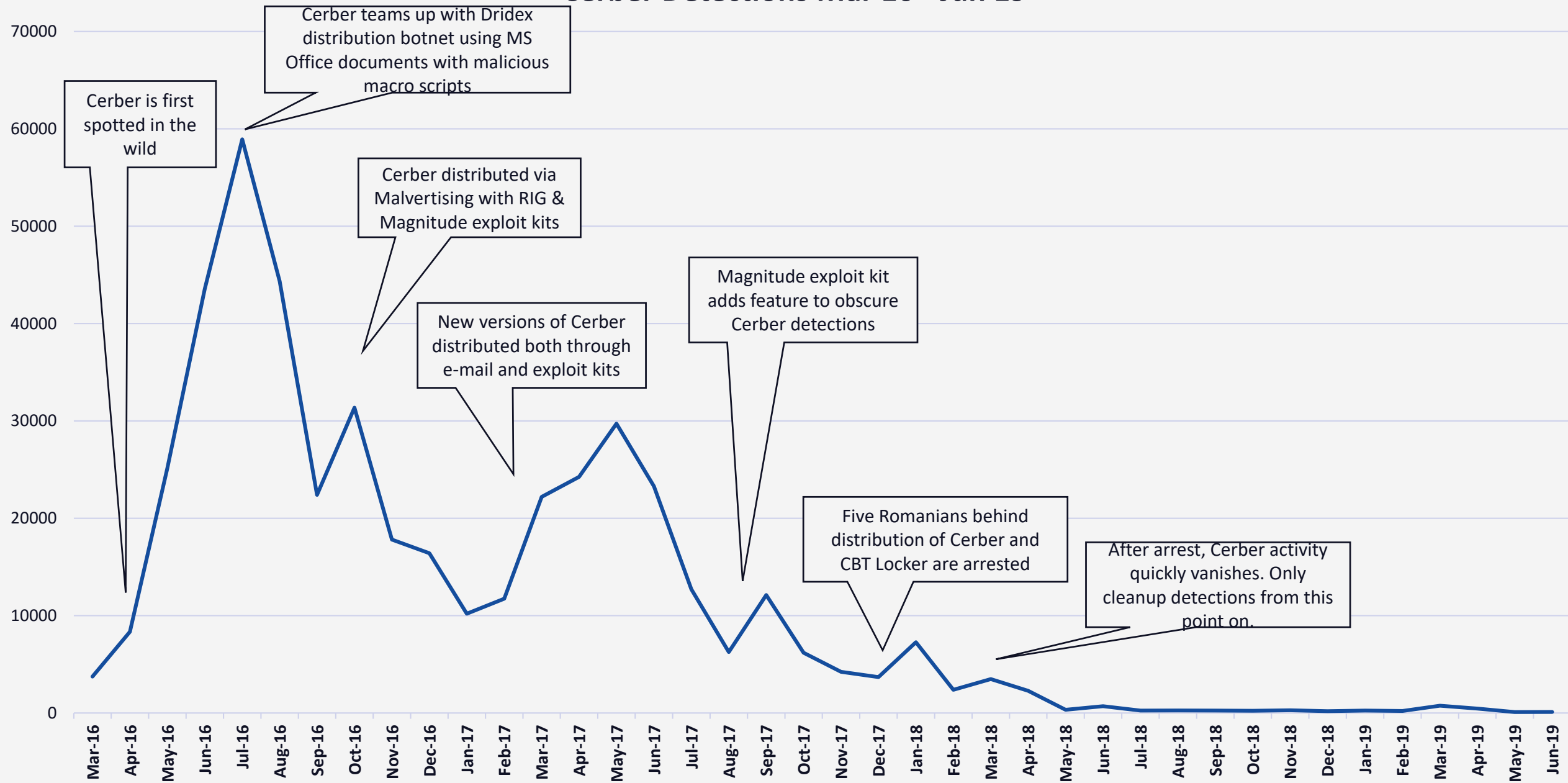
<http://ahuqfrqk54v3vnzj.5hhseo.top/B9B9-3AF4-5946-008C-110D>

<http://ahuqfrqk54v3vnzj.v4nus1.top/B9B9-3AF4-5946-008C-110D>

<http://ahuqfrqk54v3vnzj.onion.to/B9B9-3AF4-5946-008C-110D>

<http://ahuqfrqk54v3vnzj.onion/B9B9-3AF4-5946-008C-110D> (TOR)

Cerber Detections Mar 16 - Jun 19



PREDICTIONS



The Ransomware of Tomorrow



Increased use of manual infections

- » We've seen an increasing trend of manual attacks using ransomware
- » Manually disable security tools
- » Greater risk to attacker if they leave behind clues



Additional 'blended' attacks

- » We will see continued development of infection methods that work off each other.
- » Automated + manual infection attacks are far more successful



Ransomware will continue to pair up other malware

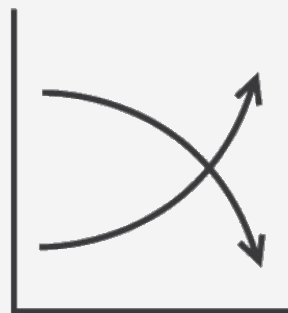
- » Much like we've seen with Ryuk, Trickbot and Emotet
- » We are near the end of the 'single purpose' malware era.

The Ransomware of Tomorrow



Additional development of infection venues

- » As we've seen with new exploits & malicious scripts over the last year
- » Infection venues will always be developed upon, to find a more effective way of attack.



Consumer facing ransomware will vanish

- » Ransomware has shown it is far more powerful against organizations
- » Ransomware focused on consumer is likely to be replaced by adware, spyware or crypto miners.



Ransomware use will continue through the year

- » The trend of using ransomware has become too popular to avoid
- » We will continue to see ransom attacks throughout the year
- » New approaches to security technology and/or proactive efforts by companies should slow this down.

Conclusion

Ransomware is here to stay, at least for a while

» Proactive protection is required

- » Detection based on behavior
- » Identification of valuable data to be better protected
- » Establishment of company wide guidance on ransomware

» It's not about if, but when

- » There are many avenues for infection when it comes to organizational networks
- » Methods that have worked for decades continue to work (i.e. spear phishing)
- » Providing users with options to report suspicious e-mails is a good first step

» Attacks are a case by case situation

- » A single method for protection from ransomware may not be viable for all organizations
- » Paying the ransom depends on the overall cost to the organization
- » Getting back up and running is paramount



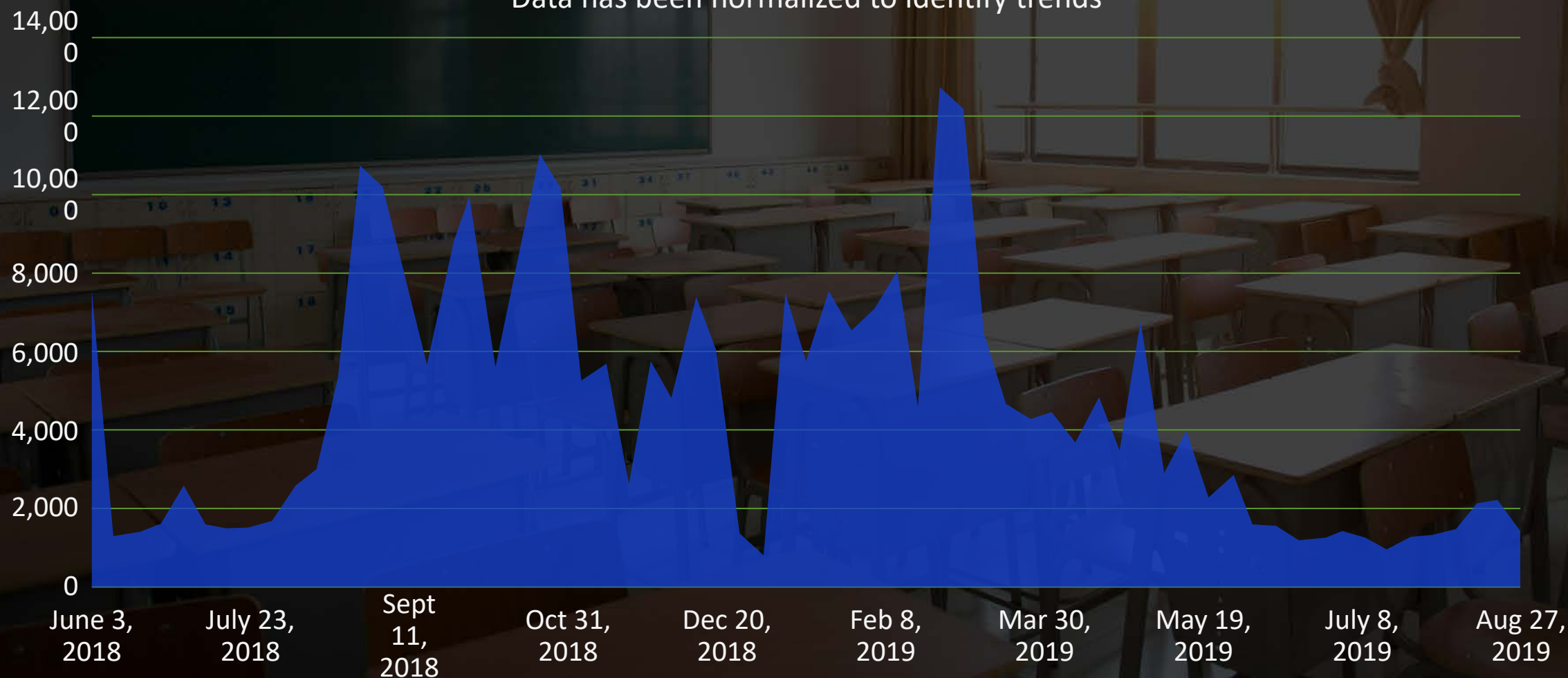
Classroom time is maximized
when your environment
is protected



The Educational Threat Landscape

Education Organization Overall Detections (June 2018–Aug 2019)

Data has been normalized to identify trends



Treasure Trove of Personal and Financial Data



STUDENT AND STAFF
PERSONALLY-IDENTIFIABLE
INFORMATION



EDUCATION TECHNOLOGY
PROVIDERS, VENDORS, OR
THIRD-PARTY SUPPLIERS



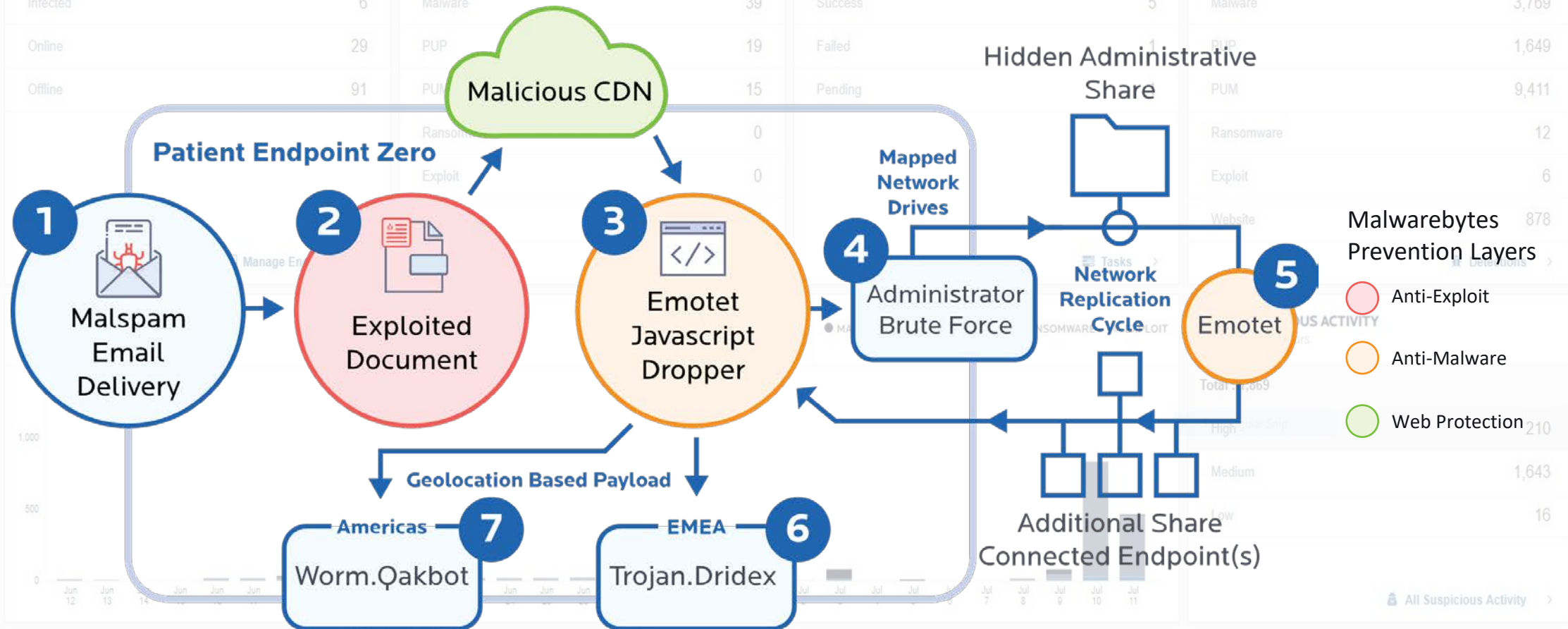
FINANCIAL INFORMATION



PUBLIC COMMUNICATION
CHANNELS AND THE
SCHOOL SYSTEM



Knowledge Share



TOP 10 ENDPOINTS WITH DETECTIONS

Past 90 Days

Name	Detections
plee-QA-W10Prox64	1,461

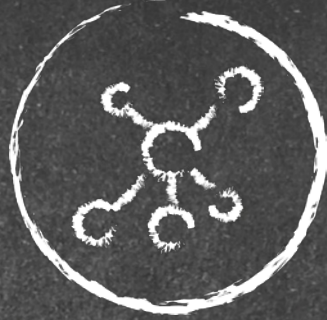
TOP 10 SUSPICIOUS ACTIVITY DETECTION RULES

Past 24 Hours

Name	Count
Hosts File Change	1,433



Securing
the cloud



Segmenting
networks



Enable secure
remote work
over Wi-Fi



Employee and
student awareness
training



Personal
apps



BYOD
policy



Incident
response plan

A faded, grayscale aerial photograph of San Francisco, showing the city skyline, the Golden Gate Bridge, and the surrounding water and hills. The image serves as a background for the title text.

Malwarebytes: Addressing Today's Threat Landscape

Malwarebytes: The Most Trusted Name in Security

BY THE NUMBERS



500k
Downloads
Per Day



3M Remediation
Events Per Day



Global
Research Team



~25% Growth YoY
35% R&D Spend

\$150M -
\$200M

Run Rate
Business, Cash
Flow Positive



Tens of Thousands
of Business
Customers

ACCOLADES



Gartner

*Gartner positions Malwarebytes in the Visionary quadrant
2018 Magic Quadrant for Endpoint Protection Platforms*

INNOVATION

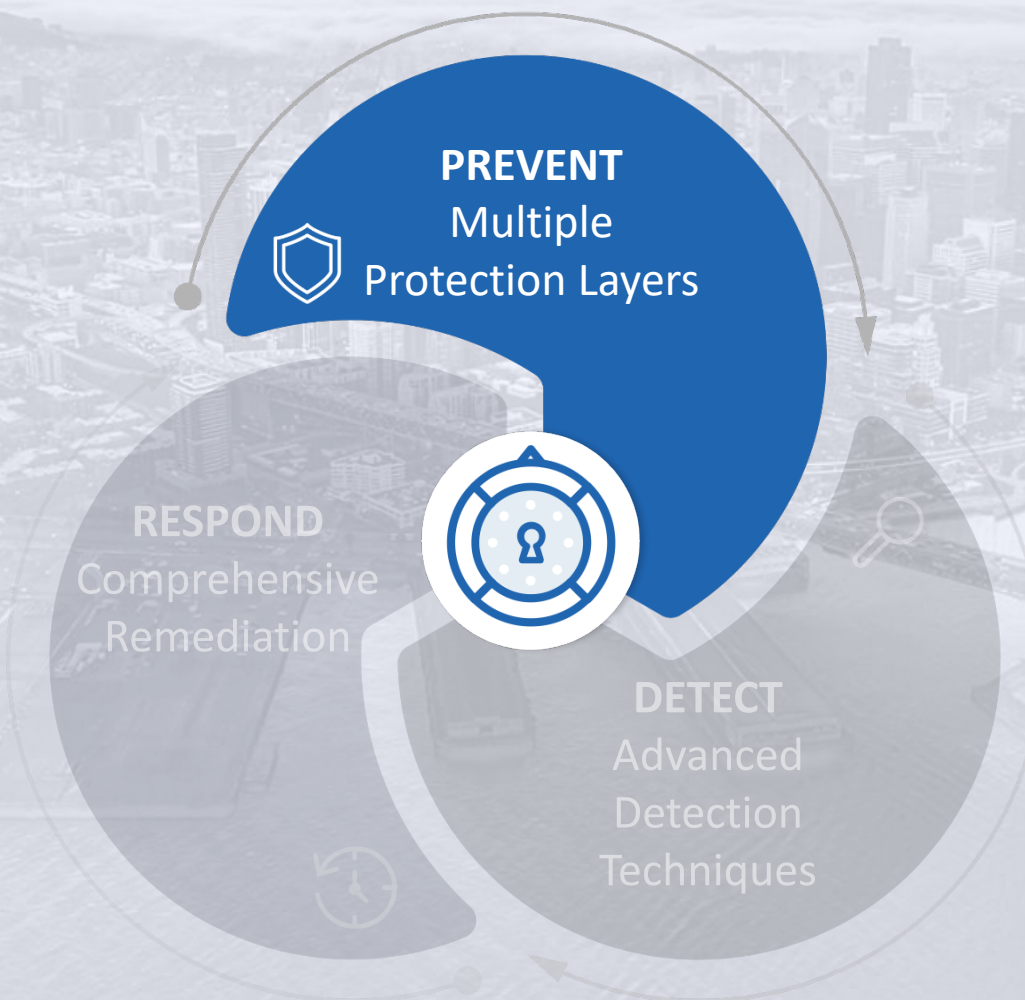


8 PATENTED TECHNOLOGIES
+ 10 PENDING

Including:

- Behavioral identification of ransomware
- Machine Learning techniques
- Fileless attack detection

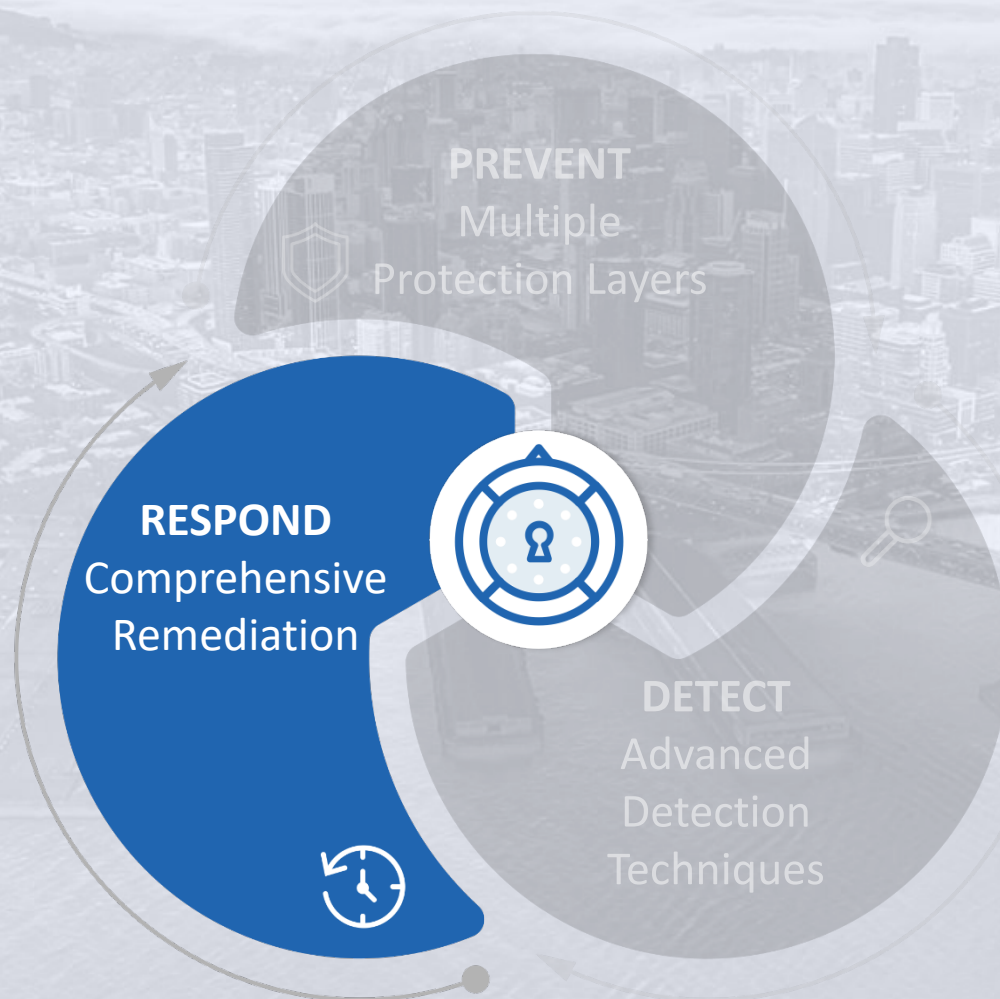
Effective Solution Components



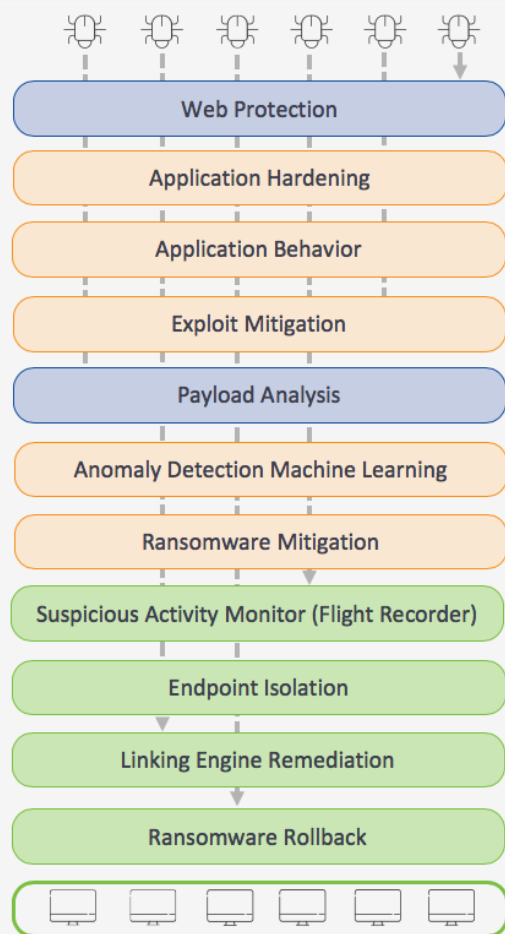
Effective Solution Components



Effective Solution Components



Malwarebytes Endpoint Protection and Response



We Don't Just Find It. We Fix It.



EDR WITHOUT COMPLEXITY



UNMATCHED THREAT VISIBILITY



**COMPREHENSIVE ATTACK
CHAIN PROTECTION**

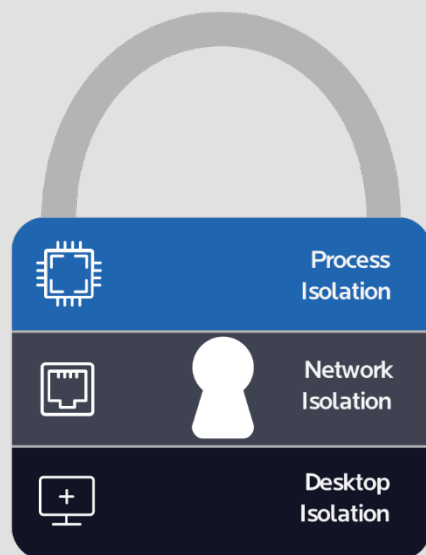


#1 TRUSTED NAME IN REMEDIATION

Protection, Detection, and Response Layers

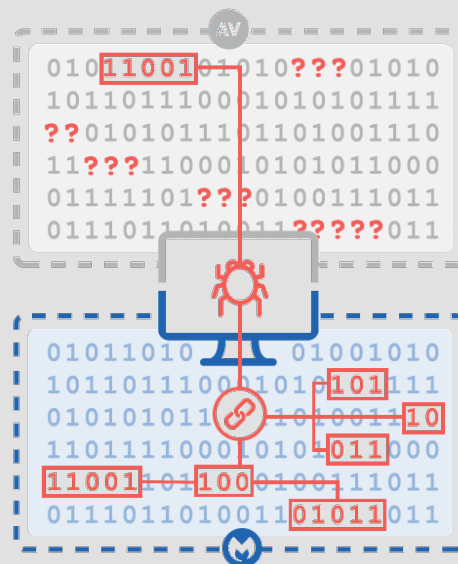
Granular Endpoint Isolation

- Isolates endpoints to stop the bleeding
- Prevents malware from connecting to C&C
- Locks remote attackers out



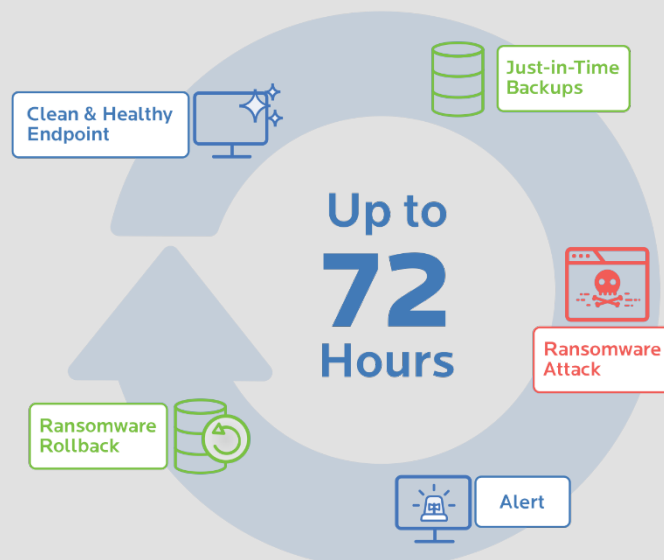
Thorough Remediation

- Cleans up primary payload
- Detects and removes all dynamic and related threat artifacts
- Minimizes end-user impact



Ransomware Rollback

- Performs just-in-time backups of file changes
- Logs/associates changes with specific processes
- Rollback damage up to 72 hours



Let's Take Your Questions

Try Now: malwarebytes.com/business/trial

Learn More: malwarebytes.com/business

See What Others Miss: malwarebytes.com/remediationmap





THANK YOU