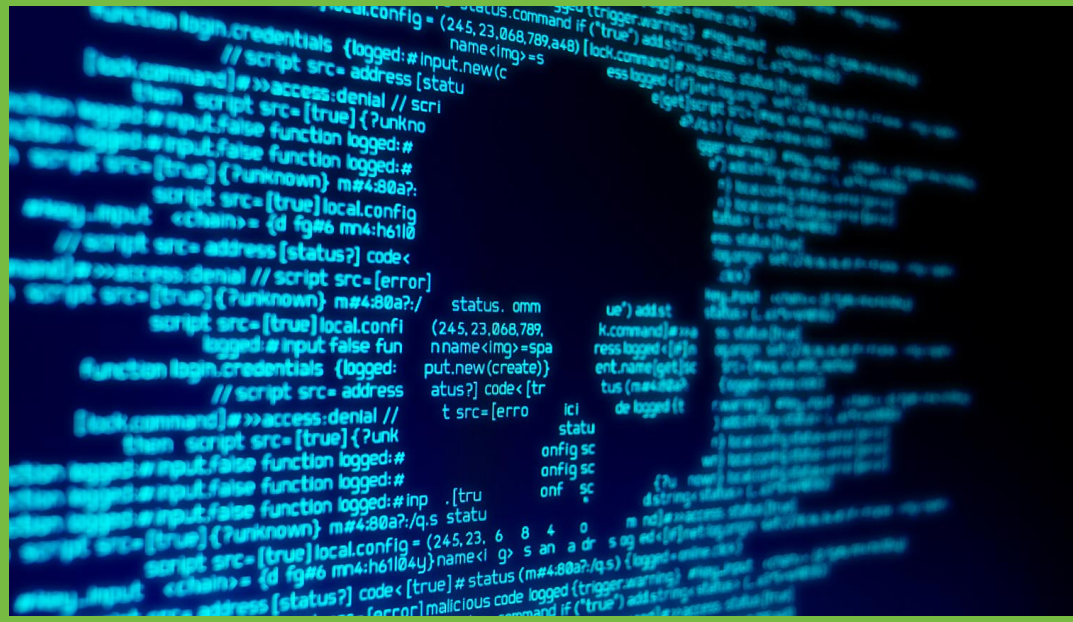
ASMGi

Malwarebytes

Why are businesses getting hit with so much malware?



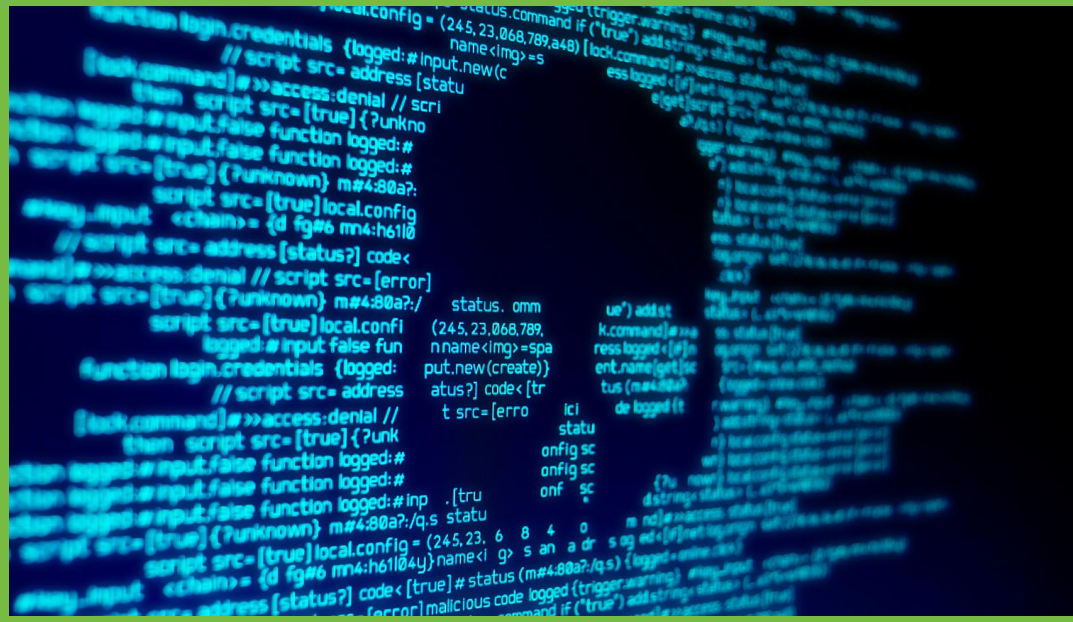
October 3, 2019

ASMGi

Malwarebytes

The Webinar Will Begin In 3 Minutes

Why are businesses getting hit with so much malware?



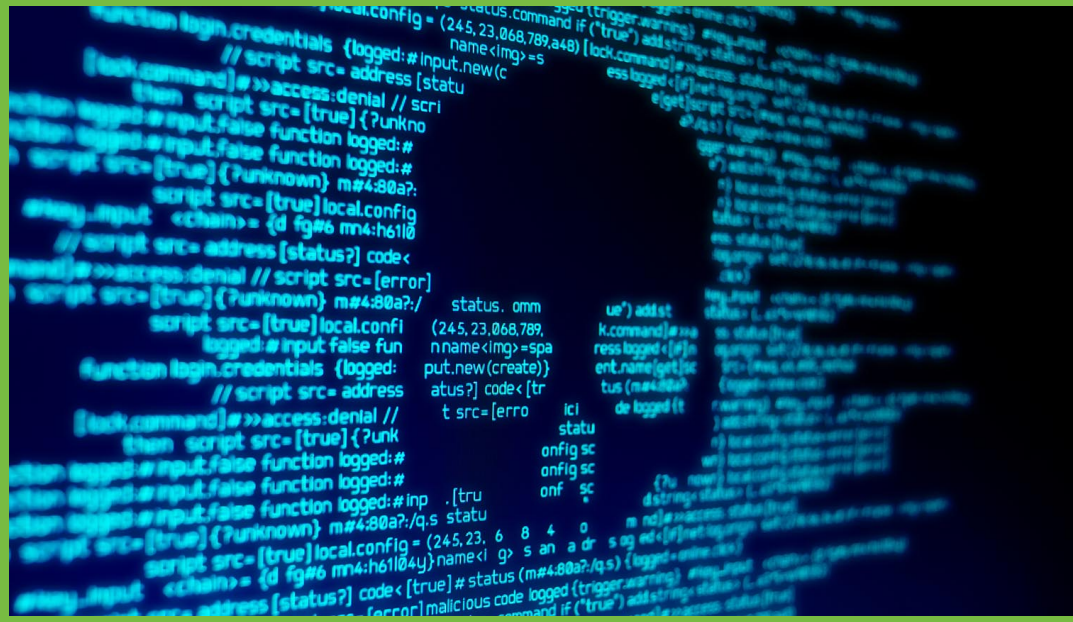
October 3, 2019

ASMGi

Malwarebytes

The Webinar Will Begin In 2 Minutes

Why are businesses getting hit with so much malware?



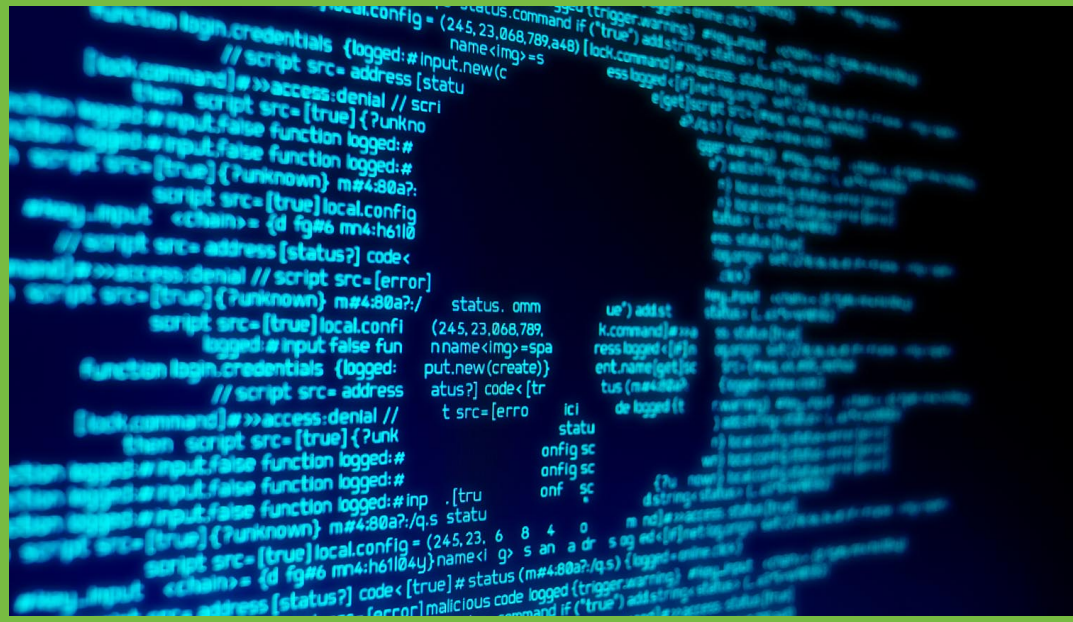
October 3, 2019

ASMGi

Malwarebytes

The Webinar Will Begin In 1 Minute

Why are businesses getting hit with so much malware?

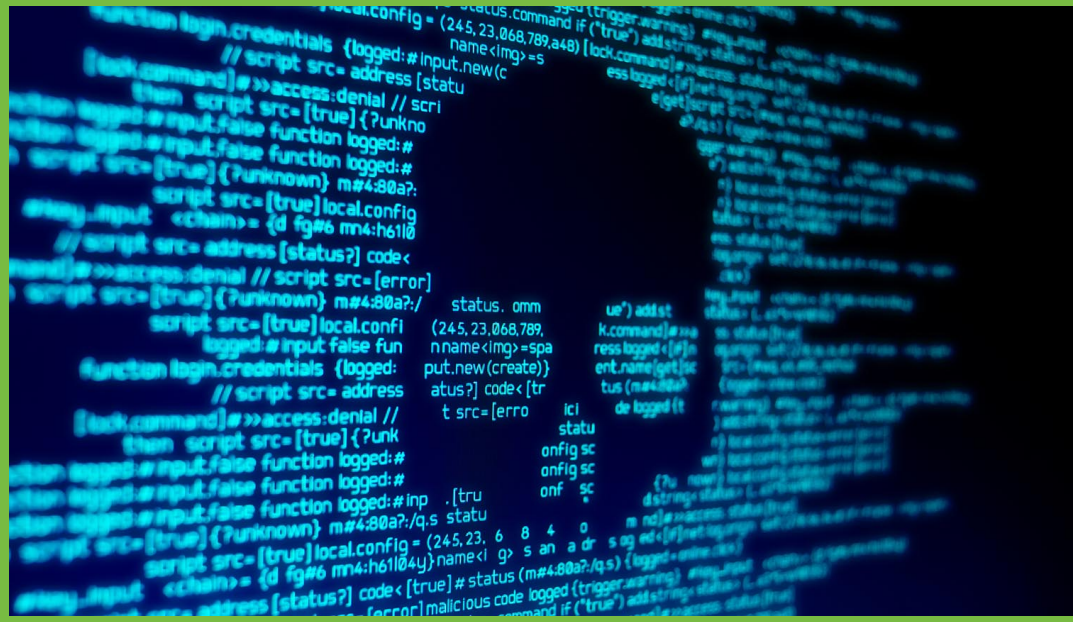


October 3, 2019

ASMGi

Malwarebytes

Why are businesses getting hit with so much malware?



October 3, 2019

Today's Presenters

Why are businesses getting hit with so much malware?

Steve Roesing

President, CEO, ASMGi

sroesing@asmgi.com

Adam Kujawa

Security Evangelist and a Director of Malwarebytes Labs

akujawa@malwarebytes.com

What is Malware?

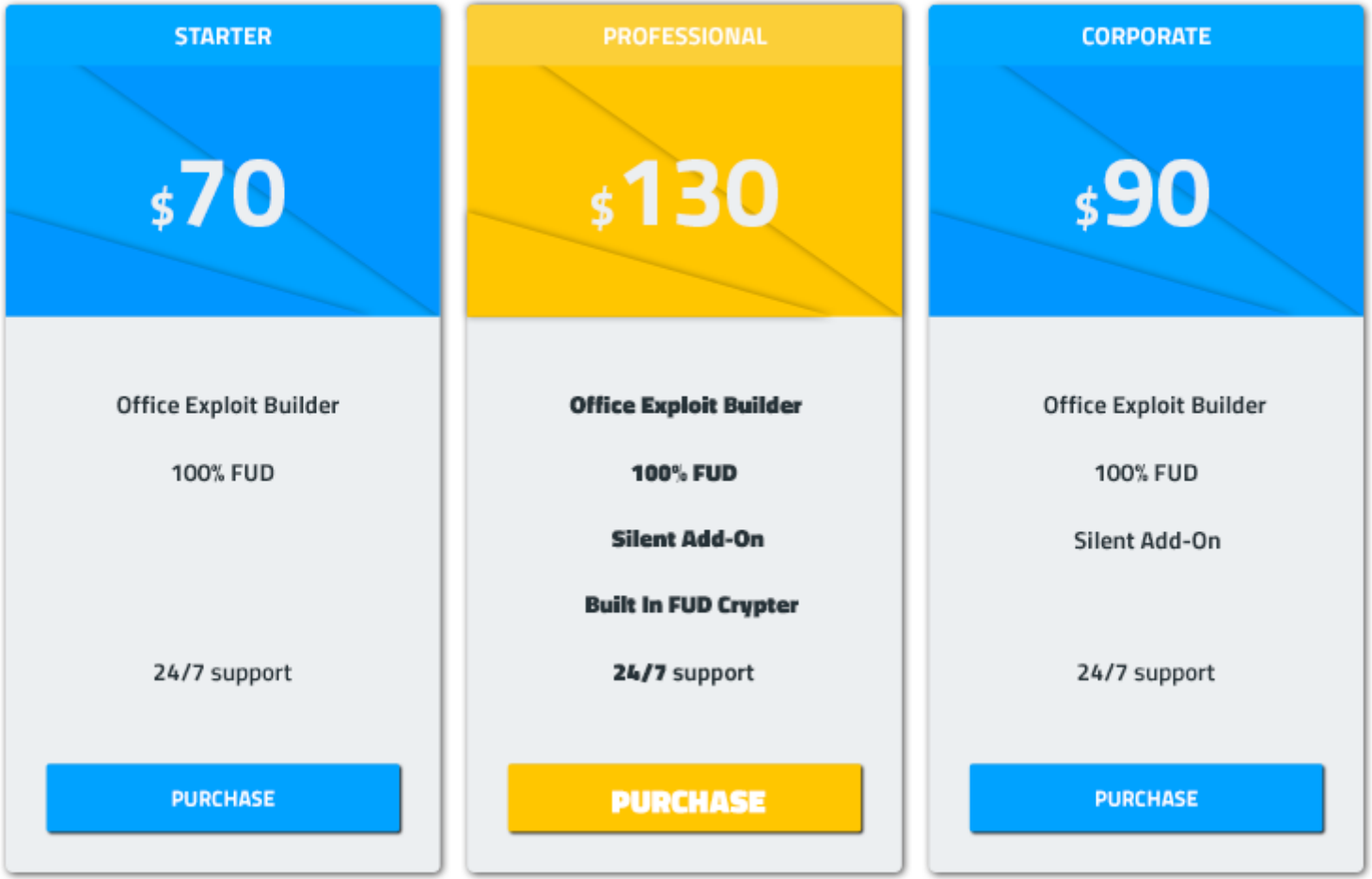
ASMGi

From Wikipedia … *Malware* *(a portmanteau for* ***malicious software****) is any software intentionally designed to cause damage to a computer, server, client, or computer network.*

So why are business getting hit with so much malware?

ASMGi

Malware Markets

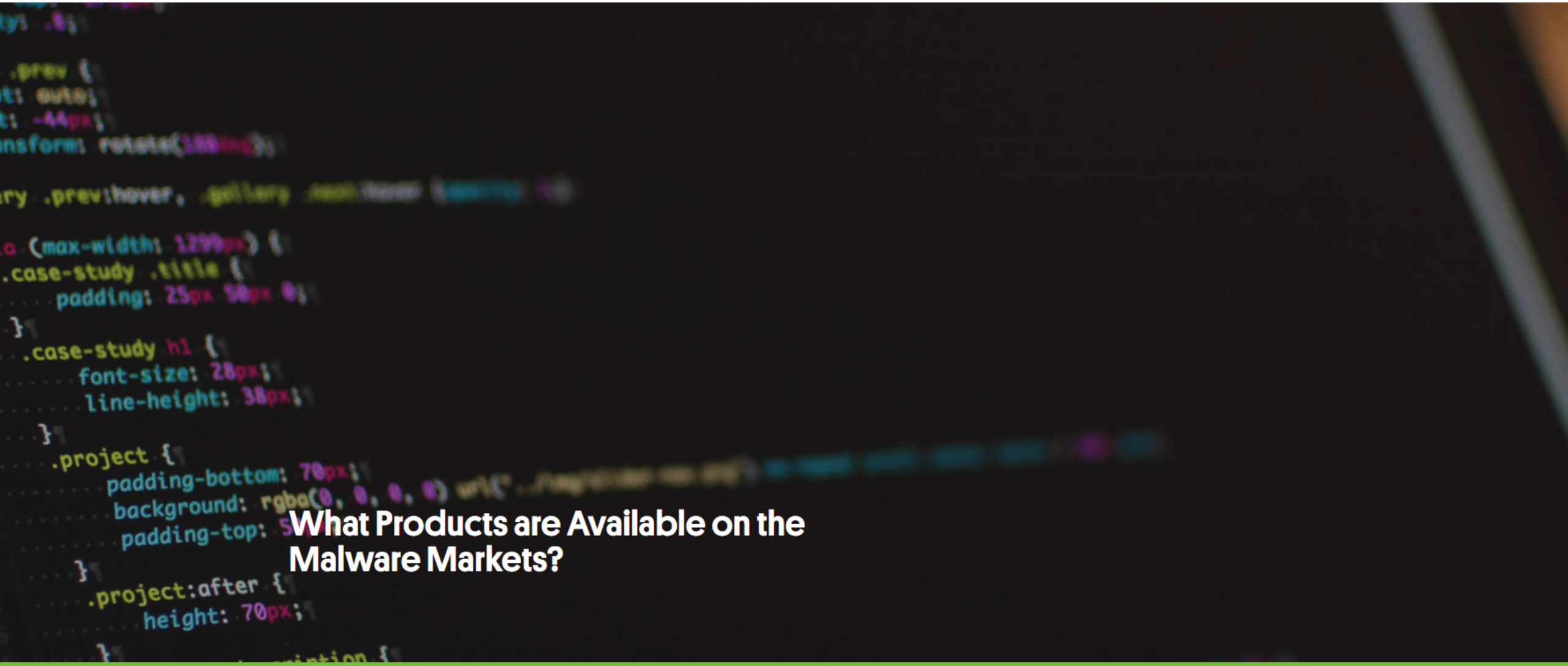


What Are the Malware Markets?

Malware Markets

A malicious software (malware) market is a network of organizations, individuals, and websites where malicious software is bought and sold. In these networks, monetization is key—profit often drives participation and participant behavior. These markets play host to services, in the form of customer support for products like botnets and offers to integrate different malware products into streamlined services. **Popular malware** used to steal banking credentials, like the Zeus trojan, are available for sale alongside offers to rent out exploit kits, which combine many different software vulnerabilities as a platform to infect as many users as possible. Where a country is unable or unwilling to develop their own malicious software, for surveillance or espionage or other activities in cyberspace, they can simply buy some from one of dozens of companies around the globe. Companies like Hacking Team, an Italian firm which sells surveillance software to governments along with training and support on how to use them, have a key role to play in these markets.

From New America, "What are Malware Markets?"


What Products are Available on the Malware Markets?

Malware Products on Marketplace

ASMGi

The malware markets contain everything from simple software programs to crack passwords to companies offering governments a one stop shop for surveillance and espionage. Some of these products are highly valuable; one company, Zerodium, advertises a **$1.5 million payout** to anyone willing to sell zero day vulnerabilities in Apple's iOS operating system. NSO Group, an Israeli company that was caught having sold surveillance malware to the UAE to **monitor human rights activists**, has been valued at **more than $1 billion**. Alongside this big business are groups that **lease access to ransomware** and rent time on botnets for just **hundreds** to **thousands** of dollars a week. This dichotomy in prices and offerings has helped create a **two-tiered market**, with a larger lower level conducting business in online marketplaces, and a small upper level working through social networks and encrypted communications.

From New America, "What are Malware Markets?"

ASMGi

Future of Malware Markets

ASMGi

All this specialization and market interaction is trouble enough today but what might be around the corner? One worry is the automation of development for new malware variants. Using machine learning techniques on par with those employed by defenders to identify and take apart malware, attackers could churn out thousands of functionally distinct samples a day. No longer the small changes designed to fool intrusion detection and prevention systems, these variants could each vary in purpose and design, overwhelming defenders. Groups might offer these automated assembly lines up for rental or sale to the highest bidder with competition driving innovation in new features and capabilities.

Currently, few malware kits and tools target embedded systems like DVRs or automobiles, but that is going to change. As disruptions like the **Mirai botnet** show, the Internet of Things is a large and growing underbelly to the digital landscape that's proving incredibly vulnerable. As participants in the malware markets find ways to monetize this vulnerability, the stakes will go up. Imagine ransomware that locks you out of your car, your house, or a critical medical device like a dialysis machine. Now consider what it looks like when the tools used to build that ransomware are leaked and available all over the internet.

From New America, "What are Malware Markets?"

Future of Malware Markets

ASMGi

Attackers Outpacing Defenders

Improved machine learning techniques could allow malware authors to produce hundreds of thousands of new version of their code each day. Each new variant might come with a different design and new functions, inundating defenders. Machine learning is used on defense as well, aiding with malware identification and forensics. The question is, who can integrate these tools and adapt faster?

From New America, "What are Malware Markets?"

How do we win…

ASMGi

Adapt to the threat

Your organization's success depends on endpoints being operational. Malwarebytes delivers cyber protection that creates a resilient security posture tailored to your endpoint environment. And because advanced, polymorphic threats are targeting the endpoint with adaptive techniques, we use multiple layers of technology applied at various points along the attack chain—including machine learning–enhanced and heuristic detection capabilities—to crush their attacks.

Malwarebytes Endpoint Protection

Respond, deliberately

Responding to a threat requires speed and know-how. Malwarebytes allows security professionals to actively and quickly respond by isolating an attack in progress and automating the remediation and recovery of the impacted endpoint. Our endpoint detection and response technology saves precious time typically spent hunting for the threat, and returns endpoints to operation without costly re-imaging.

Malwarebytes Incident Response

Malwarebytes Endpoint Protection and Response

A Holistic Approach to Cyber Security

ASMGi

Total Solution = Program + Technology + Operations

Create a Technology Ecosystem…

ASMGi

Technology partner integrations

Integrate Malwarebytes endpoint solution platforms with your security and IT ecosystems for simpler processes, faster responses, and continuous business productivity. Partner up for stronger cyber resilience.

Malwarebytes

Why are businesses getting hit with so much malware?

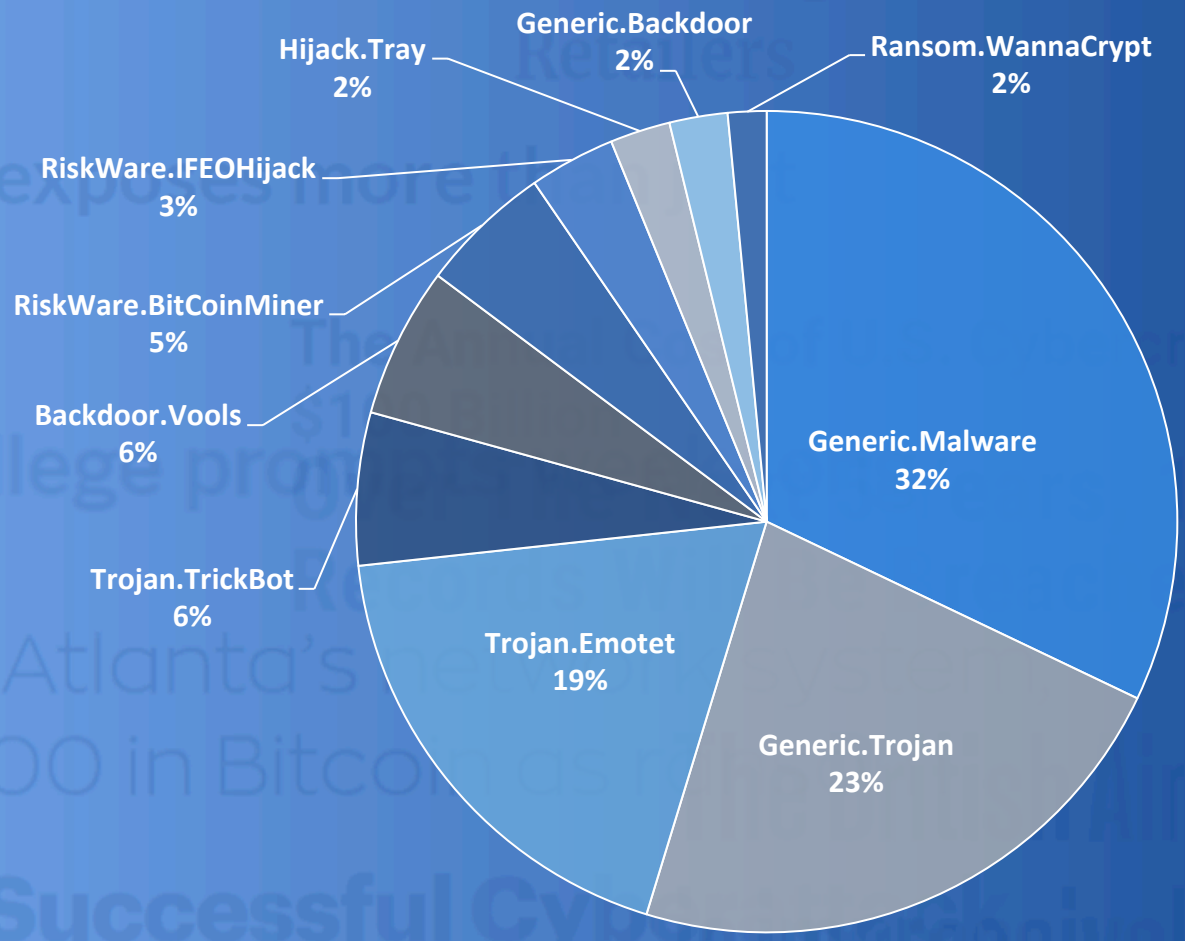
All the threats are on the rise!

BUSINESS DETECTIONS 2017/2018

Pos.	Threat	Y/Y% Change
1	Trojan	132%
2	Hijacker	43%
3	Riskware Tool	126%
4	Backdoor	173%
5	Adware	1%
6	Spyware	142%
7	Ransom	9%
8	Worm	-9%
9	Rogue	-52%
10	HackTool	-45%

Overall Detections		
2017	39,970,812	79%
2018	71,823,114	

Breaking Down the Top Threats of 2018

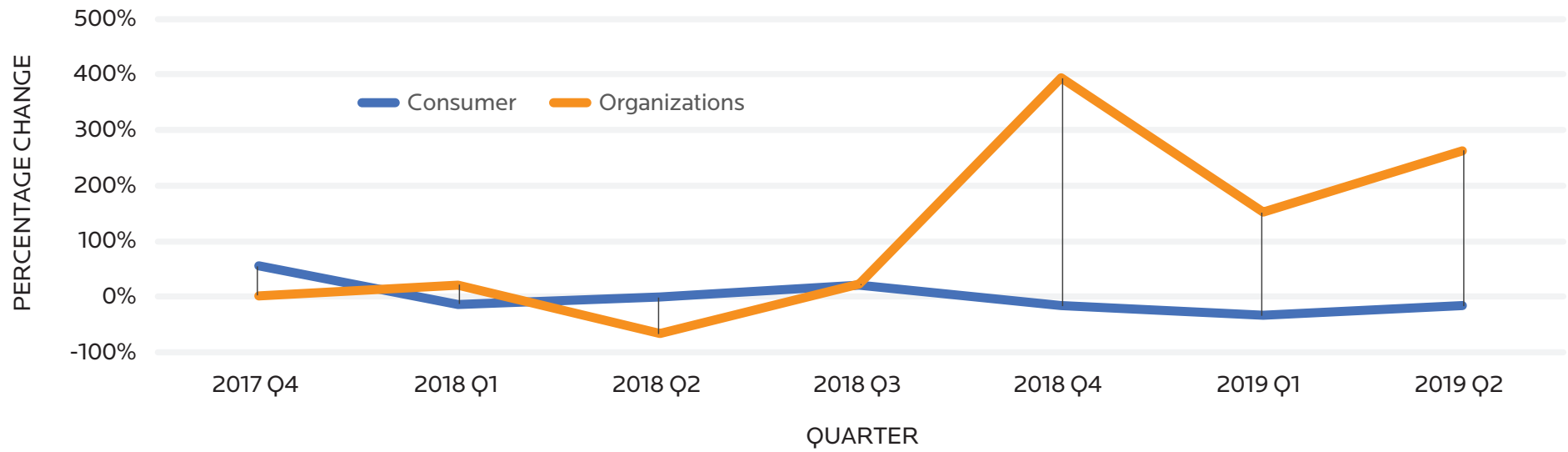


Business PRODUCT RANSOMWARE DETECTIONS 2018 - 2019

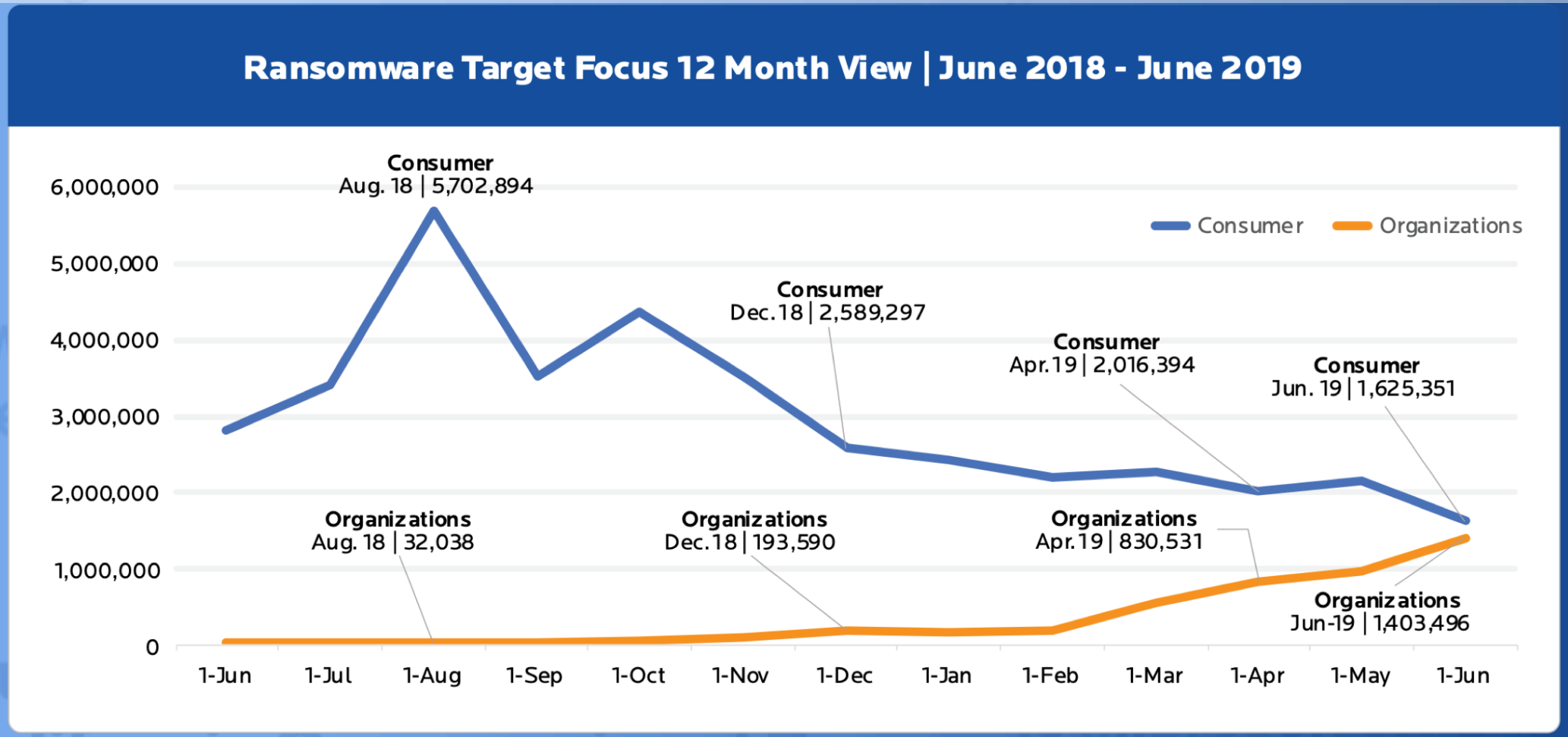
Ransomware Family	YoY % Change 2018-2019	QoQ % Change Q1 - Q2
All Ransomware	**363%**	**14%**
GandCrab	NEW	88%
Ryuk	24%	-5%
Troldesh	NEW	-47%
Rapid	NEW	940%
Locky	319%	19%

	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



Why the shift?

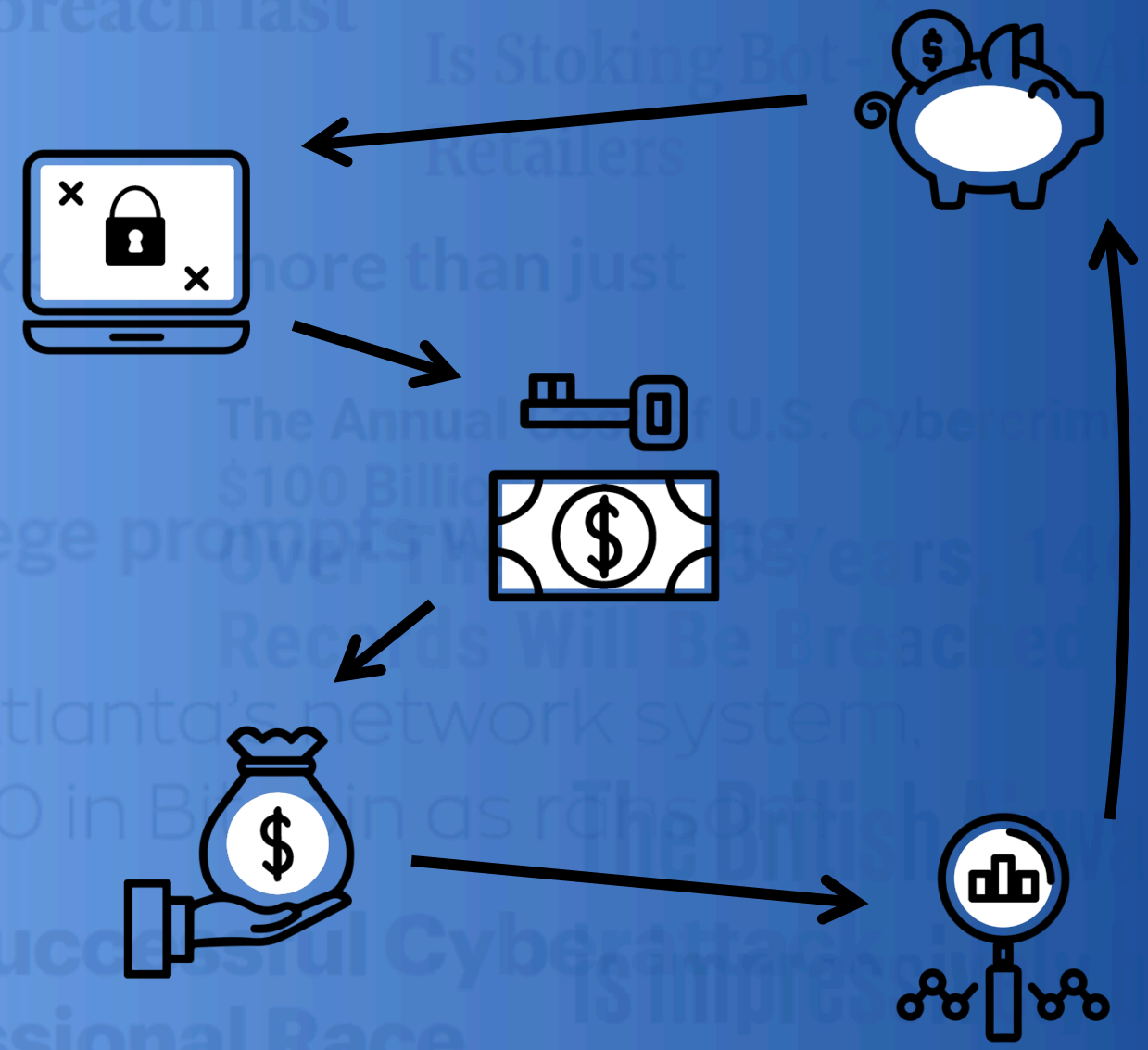
Business attacks have surged in 2019

- 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
- Higher chance of return



Why the shift?

New Technologies

» EternalBlue

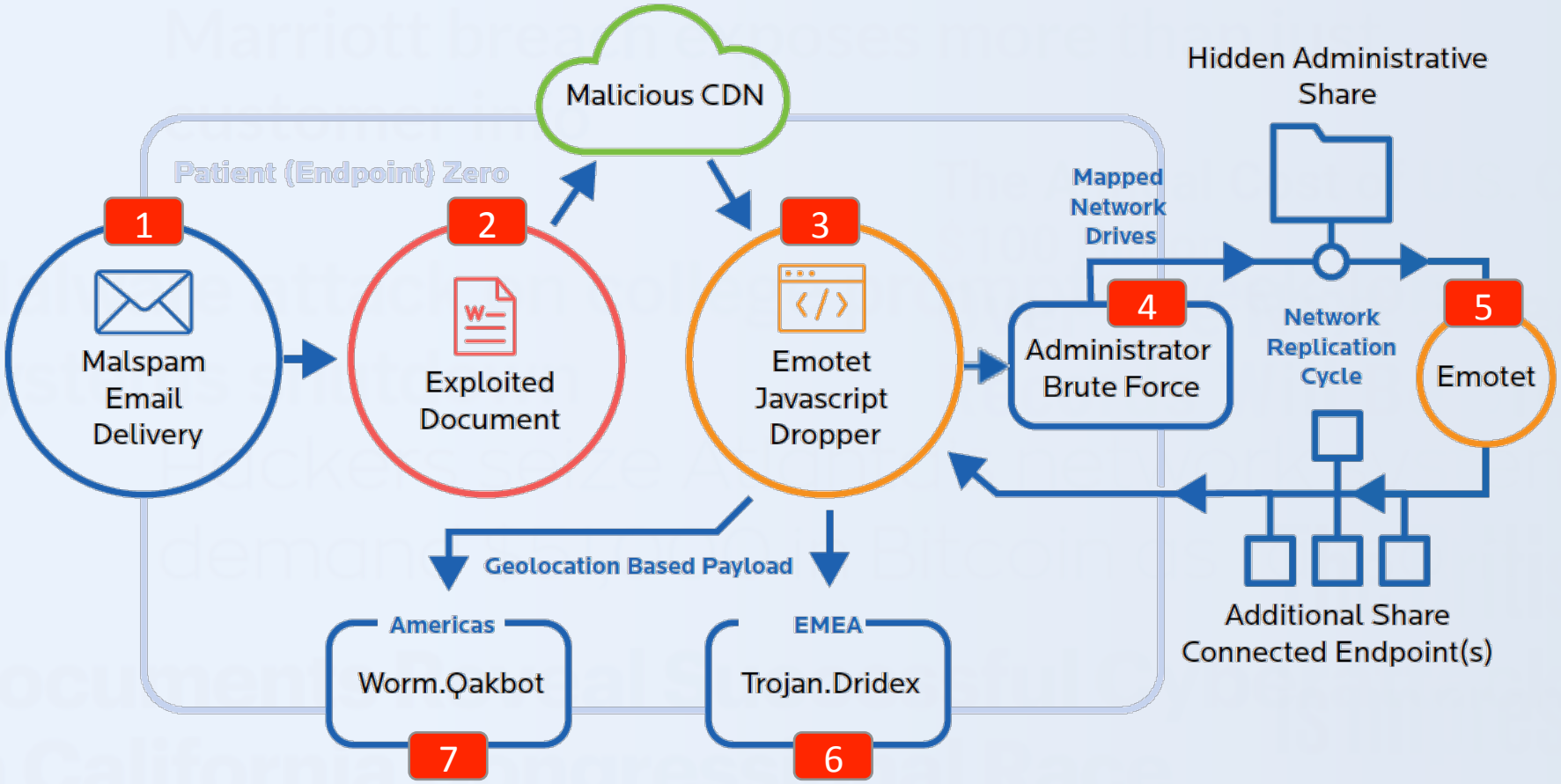
» WannaCry & NotPetya

» TrickBot & Emotet

RETURN ON INVESTMENT BREAKDOWN

Category	Considerations	Business	Consumer	Values	
Attack Opportunity	Choice of Manual Infection	2.00	1.00	Low	1.00
	Infection Entry Points	3.00	1.00	Low - Mid	1.50
	Lateral Movement Benefits	3.00	1.00	Mid	2.00
	Size of Campaign Targets	1.50	3.00	Mid- High	2.50
	Systems Targeted	3.00	1.00	High	3.00
	Varian Re-Use Ability	2.50	1.50		
	Sub Total	15.00	8.50		
Value	Value of Files to Ransom	3.00	1.50		
	Ransom Payment Demand Value	3.00	1.50		
	Value of Additional Infection	2.50	1.00		
	Value to Cost of Ransomware (Price / Dev Time / Re-Use)	2.00	2.50		
	Value of Media Attention	2.50	1.50		
	Value of Cost of Infection / Targeting	2.00	2.50		
	Sub Total	15.00	10.50		
Victim Selection	Ability to Pay	2.50	1.50		
	Chance of Encountering Defenders with LOW Ability/ Experience to Stop Attack	1.00	3.00		
	Chance of Encountering Security	2.50	1.50		
	Chance of Victim having Cyber Insurance	2.00	1.00		
	Lack of Option (Pay / Not Pay)	2.50	1.50		
	Negative Fallout from Ransom	3.00	1.00		
	Sub Totals	13.50	9.50		
	Grand Totals	43.50	28.50		

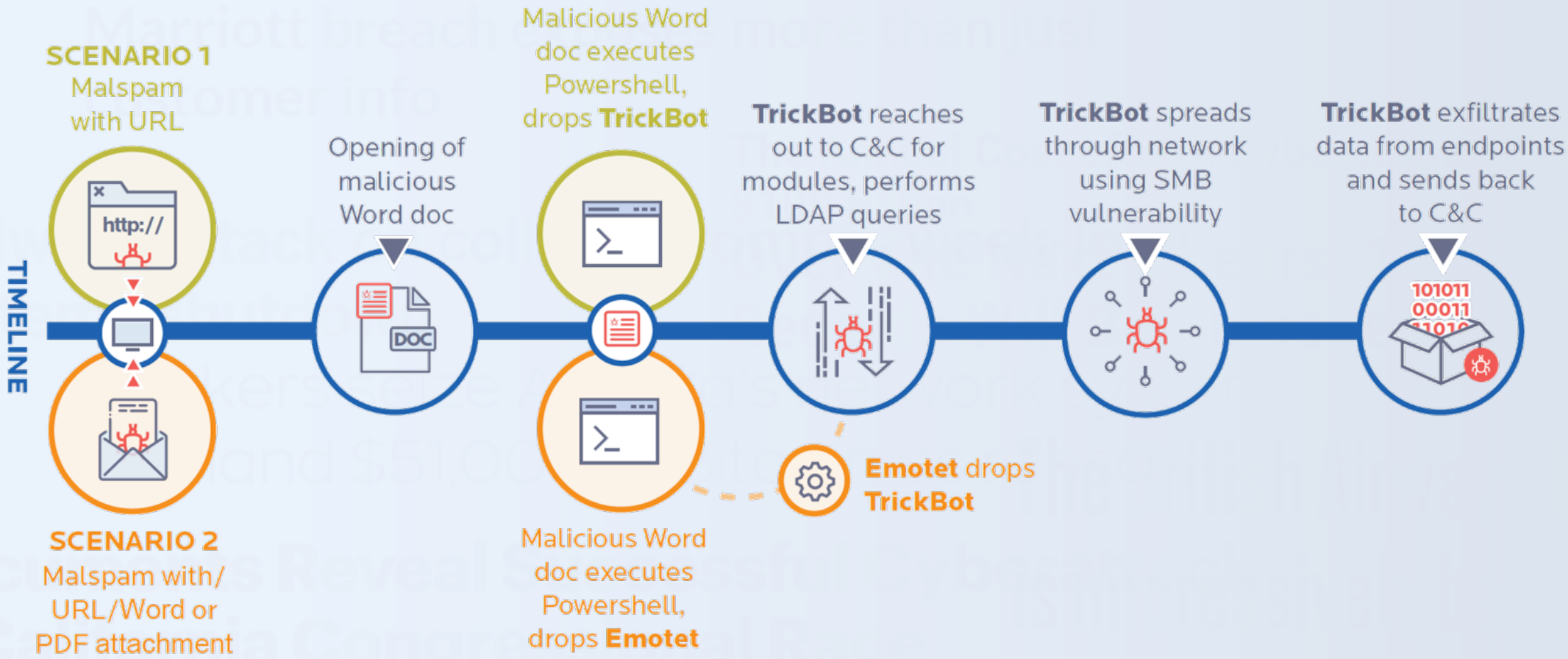
Why Emotet Is So Effective



MALWAREBYTES PREVENTION LAYERS:

- Anti-Exploit
- Anti-Malware
- Web Protection

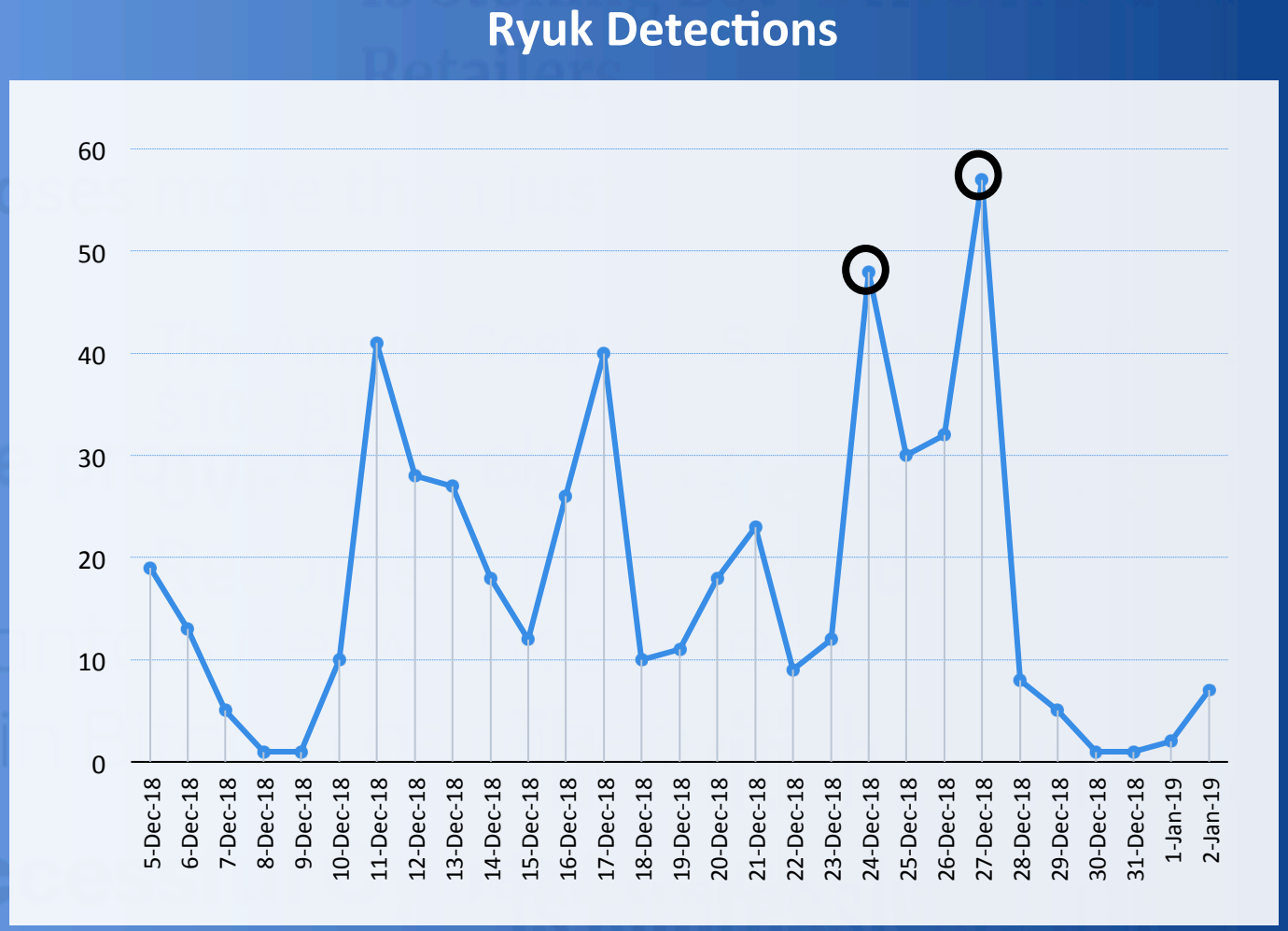
How TrickBot Works



Ransomware

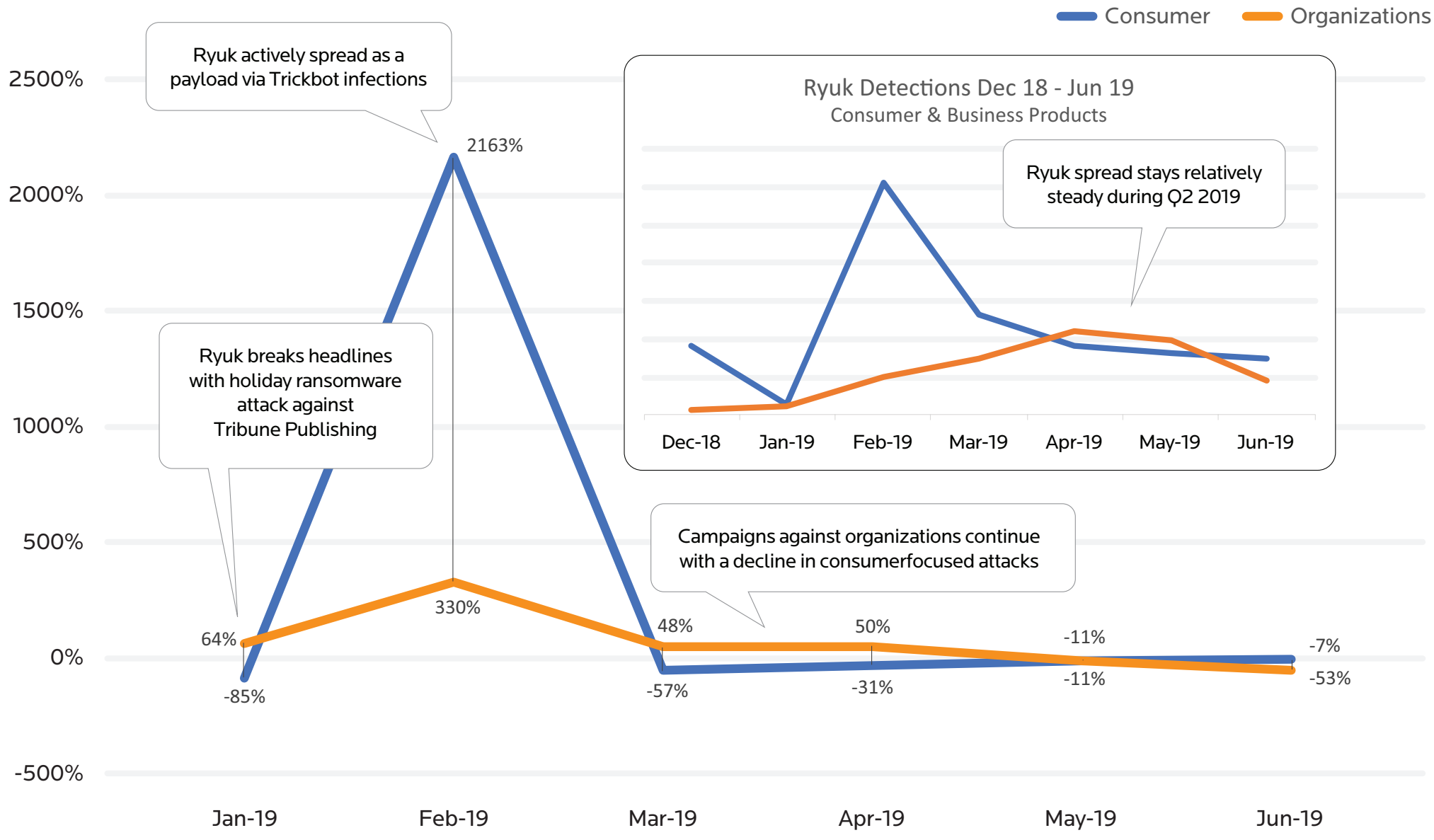
Ryuk

- First seen in the wild in 2018
- Used to attack Water Authorities, Cloud Backup Sites, etc.
- Based on Hermes Ransomware
- Holiday Attack Campaign
- Distributed through Trickbot after Emotet infection.
- Utilizes RSA 2048 & AES 256 encryption



Ryuk Ransomware Detections by Percentage Changes | 2019

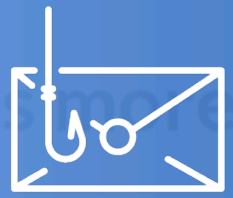
Consumer & Business Products



Beyond Security Software

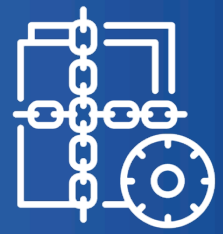
Only IT staff can install software

- Whitelisting what apps can be installed
- Using only supported applications to ensure all new updates are available



Procedure for dealing with Phishing Attacks

- Specific e-mail box for users to forward phishing e-mails
- User education on how to identify and report phishing e-mail
- Internal security / IT staff should investigate possible phishing attacks



Segmentation of valuable network resources

- Reduce damage done to the network from a single attack
- Place valuable systems / data behind additional security
- Limit access to only those users and systems that need it

What about the next year?

Increase use of manual infections

- We've seen an increasing trend of manual attacks
- Insecure RDP, Backdoor Shells, SMB vulnerabilities, etc.
- Manually disable security tools
- Greater risk to attacker if they leave behind clues

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

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

The smallest oversight could result in compromise

- Proactive protection is required
  - Detection based on behavior
  - Identification of valuable data to be better protected
  - Establishment of company wide guidance on malware, phishing, sharing, passwords, etc.
- 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
- This is the new norm
  - Immense focus on organizational targets has brought a LOT of media attention to cyber criminals.
  - This hype is going to bring in additional actors to the space who may have otherwise not been interested.
  - This is also going to accelerate the development of organizational defensive technologies too.

QUESTIONS?

Upcoming Webinars and Events

Events

- *October 21-25 -* ***Information Security Summit***
  at The Cleveland I-X Center

Webinars

- *October 17 -* ***Do You Know Where Your Data Is And Who Is Accessing?***
  presented by ASMGi and Heureka

All previous ASMGi webinars are available for viewing on our YouTube Channel

ASMGi

Thank You!

800 Superior Ave E, Ste 1050
Cleveland, OH 44114

Phone: 216.255.3040
Fax: 216.274.9647

Email: info@asmgi.com

www.asmgi.com