2020

Cybersecurity
INSIDERS

MALWARE & RANSOMWARE REPORT

CORE SECURITY
A HelpSystems Company

INTRODUCTION

Malware and ransomware are one of the most destructive security threats affecting organizations of all sizes, from SMBs to large enterprises and government agencies. Malware is continuously evolving and organizations are facing significant challenges in responding to the threat and protecting their IT environments against new types of viruses, worms, spyware, ransomware and crypto-jacking malware.

The 2020 Malware and Ransomware Report was produced by Cybersecurity Insiders and Core Security, a HelpSystems Company to reveal the latest malware security trends, challenges, and investment priorities.

Key findings include:

- Eighty-eight percent of respondents see malware and ransomware either as an extreme threat (55%) or moderate threat (33%). Very few respondents (2%) see them as no threat at all.
- A significant majority (75%) of IT security professionals predict malware and ransomware to become a larger threat in the future. That is an increase of four percentage points over last year's survey.
- Seventy-four percent expect an increase in attack frequency over the next 12 months – an increase of six percentage points since last year. A majority (79%) said an attack within the next two months is at least moderately likely. This is up three percentage points since last year.
- Cybersecurity professionals consider spear-phishing emails the single most dangerous malware attack vector at 83%, followed by web server exploits and domain spoofing (tied at 46%).
- Ransomware is impacting organizations at the business level as well as from an IT security policy and control perspective. On the business side, malware attacks caused an increase in IT security-related spending (59%, up from 52% in last year's survey) and productivity loss (57%). At the IT operations level, malware is causing system downtime (50%) and forcing cybersecurity professionals to update IT security strategy to focus on mitigation (48%).
- When asked about the most effective security solutions to combat malware/ransomware, security professionals rank anti-malware/antivirus/endpoint security solutions highest at 75%. This is closely followed by user awareness and training at 70%.

We would like to thank Core Security for supporting this unique research.

We hope you find this report informative and helpful as you continue your efforts in securing your organizations against evolving threats.

Thank you,

Holger Schulze

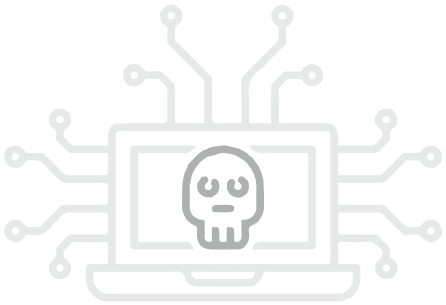
Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

MALWARE AND RANSOMWARE THREAT

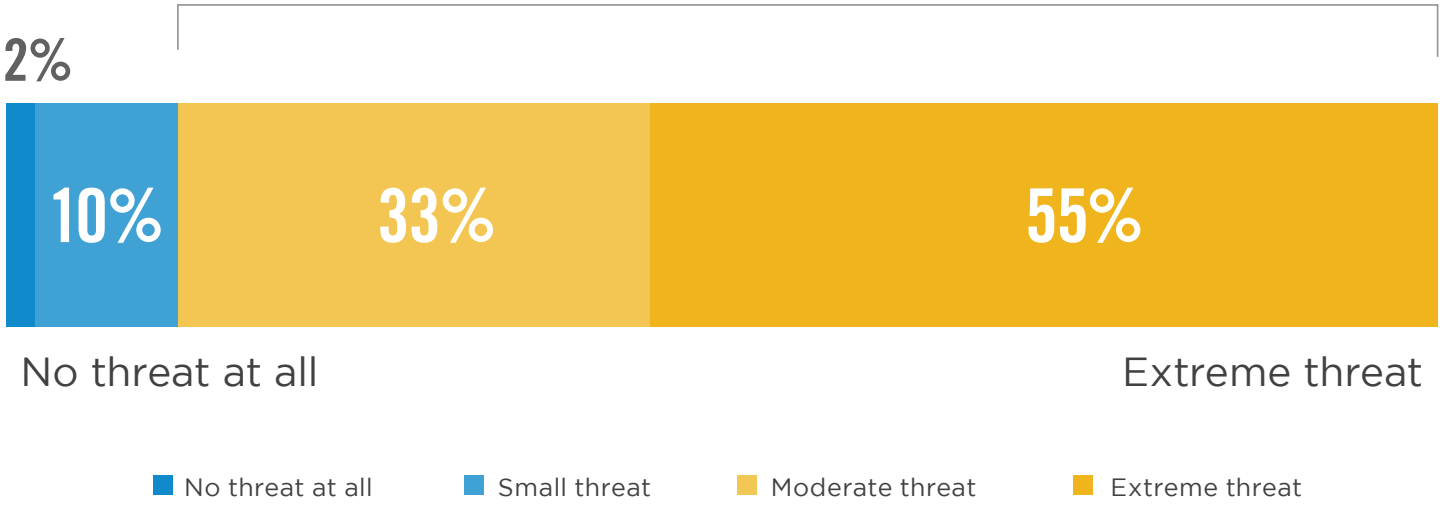
Malware and ransomware are still one of the most destructive security threats affecting organizations of all sizes, from SMBs to large enterprises and government agencies. Eighty-eight percent of respondents see malware and ransomware either as an extreme threat (55%) or moderate threat (33%). Very few respondents (2%) see them as no threat at all.

How significant a business threat is malware and ransomware to your business?



88%

Of respondents see malware as an extreme or moderate threat.



FUTURE ATTACKS

A significant majority (75%) of IT security professionals predict malware and ransomware to become a larger threat in the future. That is an increase of four percentage points over last year's survey.

Seventy-four percent expect an increase in attack frequency over the next 12 months – an increase of six percentage points since last year.

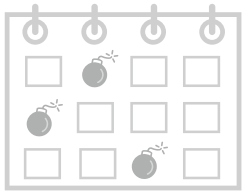
In the next 12 months, do you believe malware and ransomware will be a larger or smaller business threat to organizations?

75%

Believe malware and ransomware will be a larger threat to organizations in the next 12 months.

Are malware/ransomware attacks becoming more or less frequent overall?

74%



Believe malware and ransomware attacks will be more frequent.

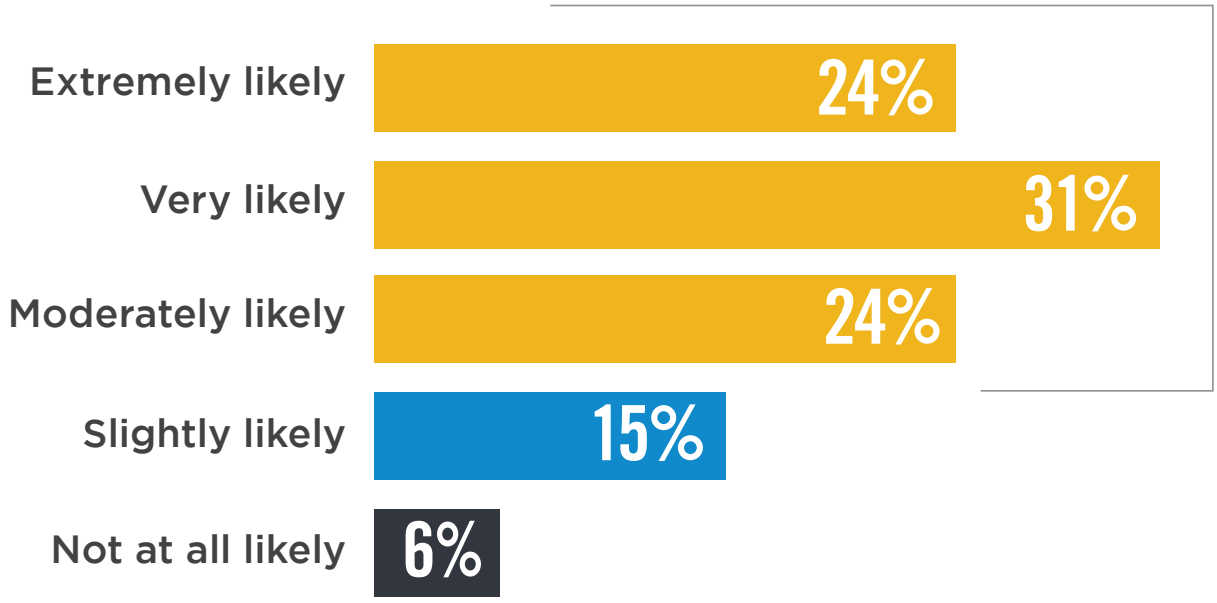
MALWARE OUTLOOK

When we asked organizations how they perceive their risk of becoming a target of malware or ransomware attacks in the next 12 months, a majority of 79% (up three percentage points since last year) said an attack is at least moderately likely.

What is the likelihood that your organization will be a target of a malware/ransomware attack in the next 12 months?

79%

Of respondents said an attack is at least moderately likely.



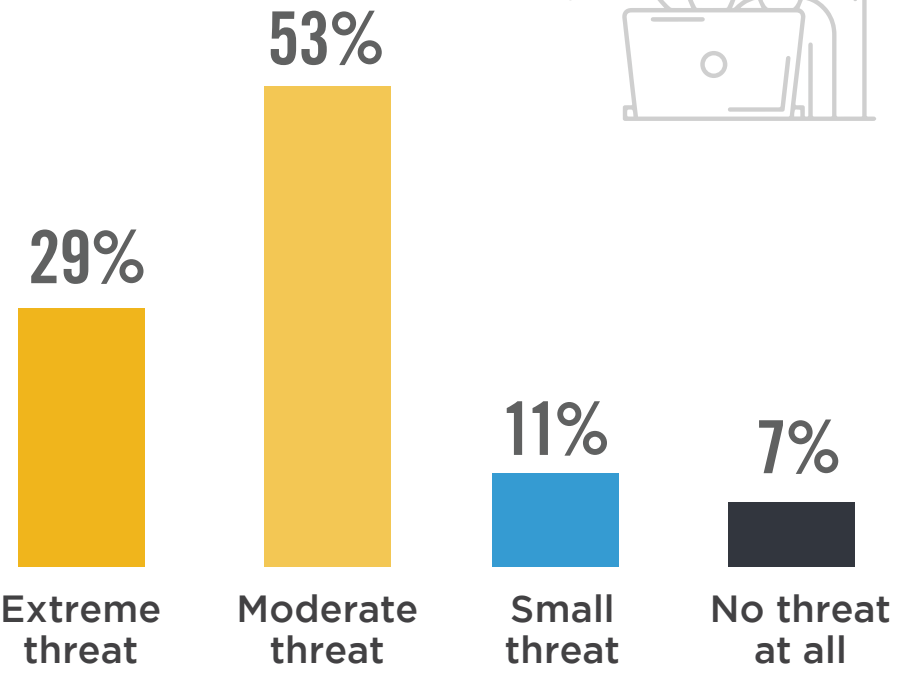
REMOTE WORK RISK

A majority of respondents (82%) view remote workers as at least a moderate threat to the business. This is a critical issue that needs to be addressed by organizations considering the massive rise in remote work arrangements in the wake of the 2020 COVID-19 pandemic.

How significant of a business threat are remote workers to your business?

82%

View remote workers as at least a moderate threat to the business.



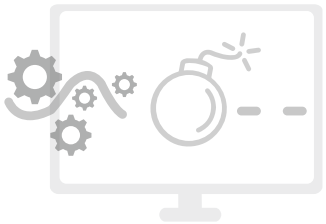
WHAT MOTIVATES ATTACKERS

Financial gain (78%) tops the list of motivators for malware and ransomware attacks. This is followed by a desire to sabotage and disrupt business activities (55%). But while money extortion is the most common motivation for cybercriminals, other motivations include hacking for fun (31%), state-sponsored attacks (28%) and political motivations (17%).

What do you believe is the main motivation for malware/ransomware attacks against your organization?

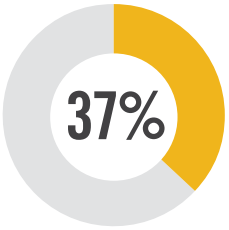
78%

Financial gain

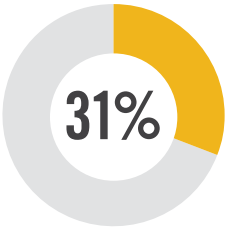


55%

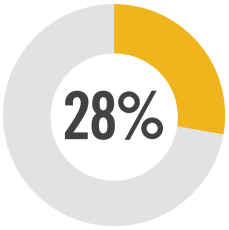
Sabotage/disruption of business



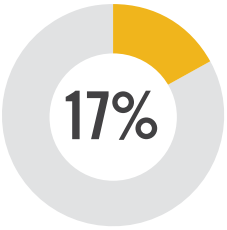
Cyber espionage



Entertainment (hacking just for fun)



State-sponsored international attack



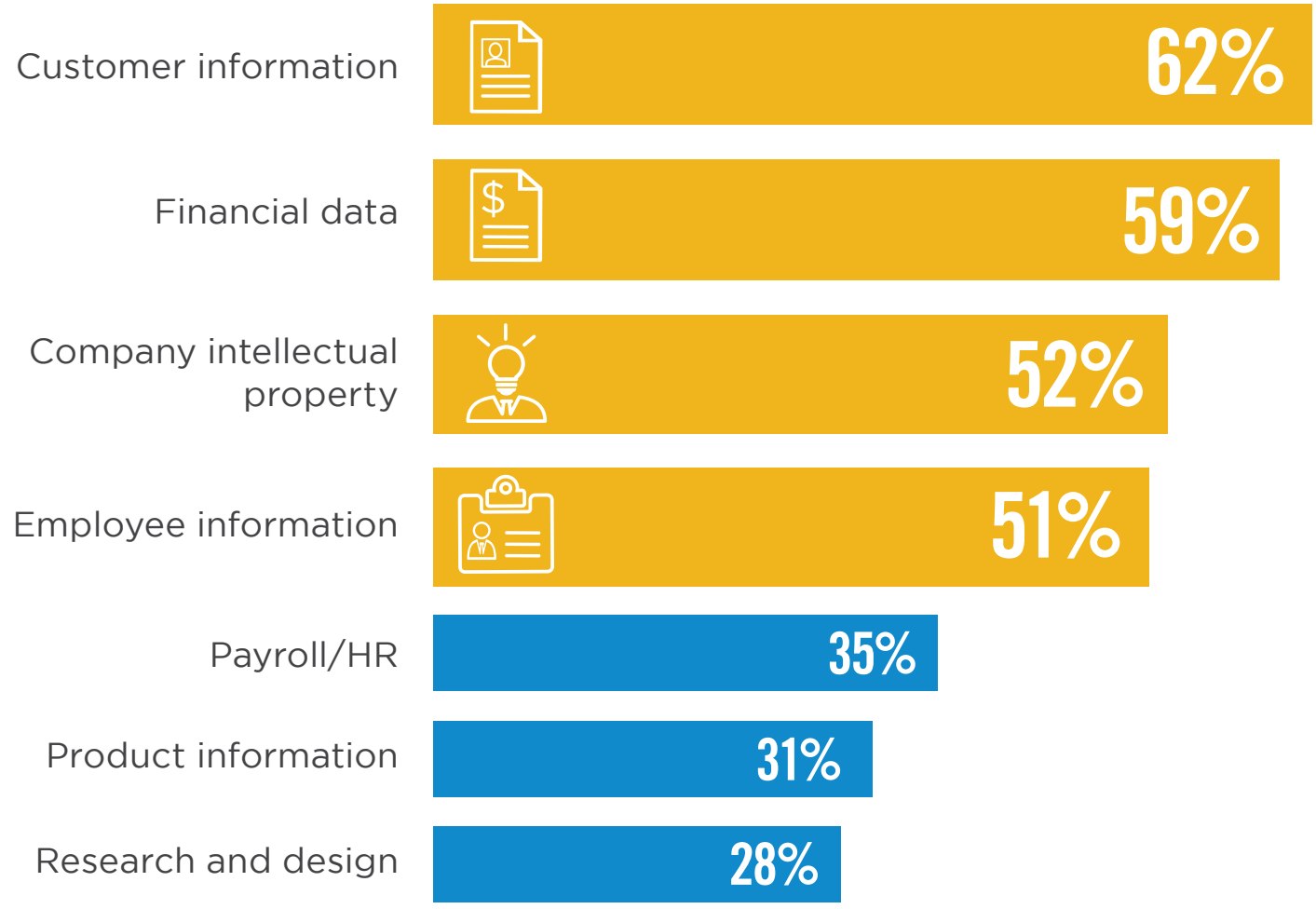
Political motivation

Revenge for a bad experience with organization 14% | Don't know/other 7%

DATA AT RISK

Data is a key strategic asset to virtually every organization and a high value target for cybercriminals. Our research reveals that the information most at risk from ransomware attacks is customer information (62%), followed by financial data (59%), and company intellectual property (52%).

What type of data in your organization is most at risk from malware/ransomware attacks?



Other 8%

MALWARE TYPES

There is a broad and ever evolving array of malware types, and new variants are created virtually every day. When asked what types of malware organizations find most concerning, ransomware is the top offender at 82% of responses, followed by phishing attacks (73%) and viruses (55%).

What types of malware are you most concerned about?

82%

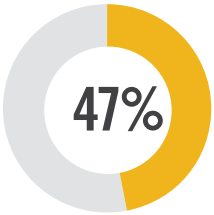
Ransomware

73%

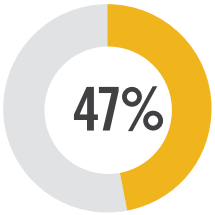
Phishing attacks

55%

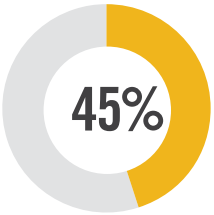
Viruses



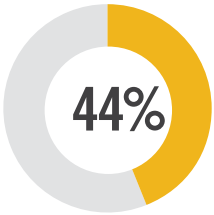
Spyware



Trojans



Rootkits



Cryptojacking

Bots 42% | Fileless malware 42% | Multi-vector malware 41% | Polymorphic malware 38% | Worms 36% | Attacks that use artificial intelligence 33% | Adware 24% | Other 2%

MALWARE ATTACK VECTORS

Cybersecurity professionals in our survey consider spear-phishing emails the single most dangerous malware attack vector at 83%, followed by web server exploits and domain spoofing (tied at 46%).

What malware attack vectors do you consider most dangerous?

83%

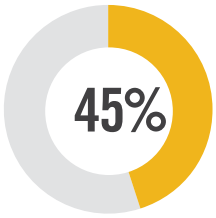
Spear-phishing emails

46%

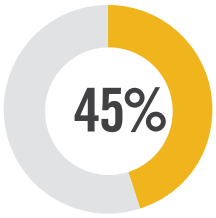
Web server exploits

46%

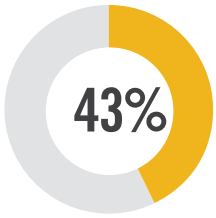
Domain spoofing



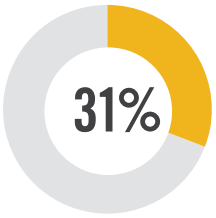
Man-in-the-middle attacks



SQL injection



Trojanized software



Watering hole websites

Cross-site scripting 30% | Other 2%

RANSOMWARE ATTACKS

More than four out of ten organizations (43%) say they experienced ransomware attacks. Fifty-seven percent of respondents have not been affected by ransomware yet or aren't aware of a previous or ongoing attack.

Has your organization suffered from ransomware attacks in the past?

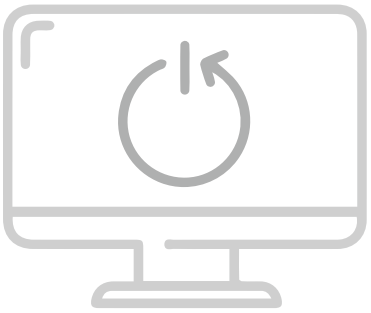
43%
YES
My organization has been affected by ransomware.

57%
NO

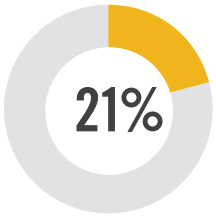
RECOVERY TACTICS

When asked how organizations recovered from ransomware attacks, a majority of 61% re-installed or restored backups. Twenty-one percent brought in third-party experts for help, and 14% managed to decrypt locked files. Only 7% paid the ransom.

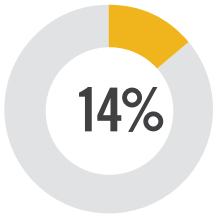
How did your organization recover from your ransomware attacks?



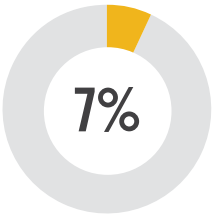
61% Re-installed/ restored



Brought in third-party



Decrypted files ourselves



Paid the ransom

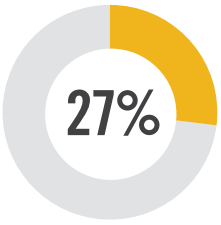
Other 33%

RANSOMWARE TYPES

There is a wide array of ransomware types and new variants are created every day. The organizations affected by ransomware overwhelmingly confirm that they encountered file encrypting ransomware as the top offender at 79% (a two percent increase of last year's survey findings).

What type of ransomware infected your organization?

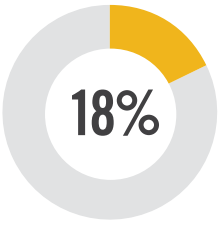
79% Encrypting ransomware or Cryptoware (encrypts files and makes them inaccessible)



Ransomware that encrypts MBR or NTFS (prevents victims' computers from being booted up in a live OS environment)

Non-encrypting ransomware or lock screens (restricts access to files and data, but does not encrypt them)

Mobile device ransomware (infects cell-phones through "drive-by downloads" or fake apps)



Leakware or extortionware (exfiltrates data that the attackers threaten to release if ransom is not paid)

Not sure/other 13%

HOW RANSOMWARE ENTERS

Survey participants report that phishing emails (68%) have taken the number one spot of entry points for ransomware, that is up by five percentage points since last year's survey, jumping up from the number two spot. Email attachments (61%) and malicious websites (46%) round out the top three most common infection methods for ransomware to gain access.

How has ransomware entered your organization?

68%

Phishing emails

61%

Email attachments

46%

Users visiting malicious or compromised websites

Exploits targeting vulnerable systems

Scan and exploit

Not sure/other 4%

IMPACT OF MALWARE ATTACKS

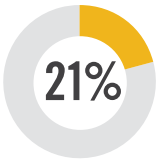
Ransomware is impacting organizations at the business level as well as from an IT security policy and control perspective. On the business side, malware attacks caused an increase in IT security related spending (59%, up from 52% in last year's survey) and productivity loss (57%). At the IT operations level, malware is causing system downtime (50%) and forcing cybersecurity professionals to update IT security strategy to focus on mitigation (48%).

What has been the impact of malware attacks on your organization in the past 12 months?

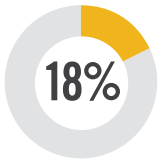
BUSINESS IMPACT

59%
Increased spending on IT security

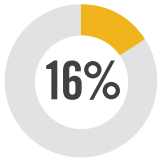
57%
Productivity loss



Revenue loss



Damage to company reputation

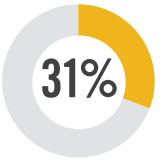


Negative press/ bad publicity

IT OPERATIONS/SECURITY IMPACT

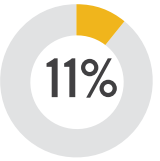
50%
System downtime

48%
Change of IT security strategy



Data loss

Loss of confidence in existing cybersecurity solutions



Senior IT staff (CIO, CISO) lost their jobs

We did not experience any ransomware attacks 7% | Other 3%

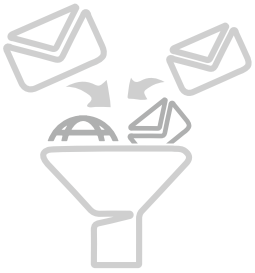
DETECTION OF THREATS

Numerous threat detection tools are available to help cybersecurity analysts identify and monitor cyber threats. The vast majority of identified malware/ransomware attacks were detected through anti-malware/antivirus/endpoint security tools (86%), email and web gateways (56%), and intrusion detection systems (56%) tied at second place. Unfortunately, an increasing number of innovative malware attacks succeed in evading detection.

How is malware/ransomware typically detected when it attempts to enter your organization?

86%

Anti-malware/ antivirus/endpoint security tools

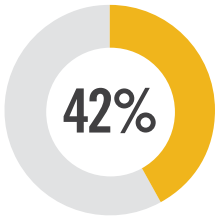


56%

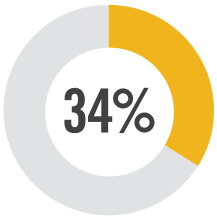
Email and web gateways

56%

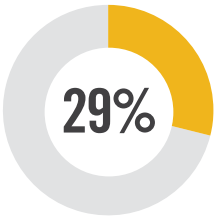
Intrusion detection system



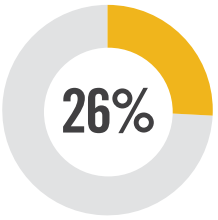
Network behavior monitoring



Detected by compromised user



User behavior monitoring



File monitoring

We cannot detect ransomware 3% | Not sure/other 5%

SPEED OF DETECTION

While the speed of malware/ransomware detection varies based on the specific strain and an organization's detection capabilities, most attacks are typically detected within hours (75%). Fifty-five percent of organizations claim detection is near real time or within minutes. The rate and speed of malware/ransomware detection is critical in combating fast moving attacks before they succeed in spreading across the network.

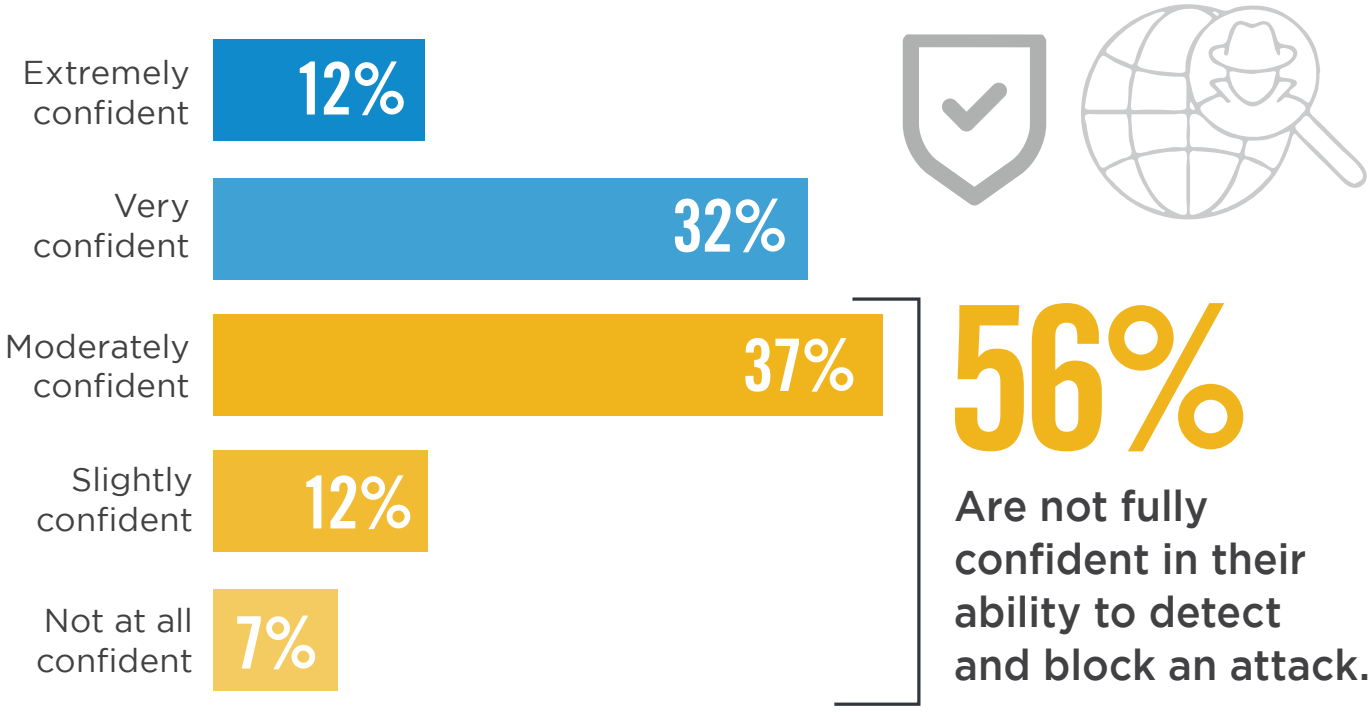
How quickly is malware/ransomware typically detected by IT security when it attempts to enter your organization?

75% Of attacks are detected within hours.

CONFIDENCE IN DETECTION

A majority of cybersecurity professionals (56%) are not fully confident in their organization's capacity to detect and block a malware/ransomware attack before it spreads to critical IT systems across the organization. Only 12% are extremely confident and 32% are very confident.

How confident are you that your organization's defenses are capable of detecting and blocking malware/ransomware before it spreads and infects critical systems and files?



CONTAINING ACTIVE INFECTIONS

How do organizations contain an active infection? About half (52%) have incident response teams and tools to detect and isolate the malware, followed by the deployment of advanced malware detection and response solutions (40%).

How does your organization detect and respond to lateral movement or infected computers that participate in a botnet?"

52%

Incident response team to detect and isolate

40%

Advanced, behavior-based malware solution that protect endpoints and has the ability to detect with automated mitigation/remediation capability

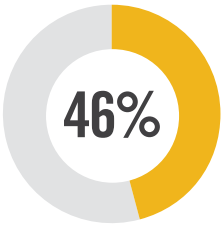
This scenario is unlikely to happen in my organization 18% | Don't know/other 22%

ATTACK RESPONSE TACTICS

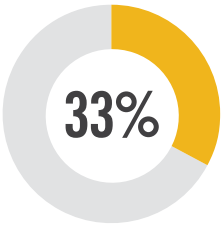
Following a ransomware attack, cybersecurity professionals deploy a number of responses. The single most common response (80%) is containing the damage by isolating and shutting down all infected systems and accounts, and recovering the encrypted files from backups while blocking the initial attack vector, if possible.

How would your organization respond when it has been detected that ransomware has attacked your systems?

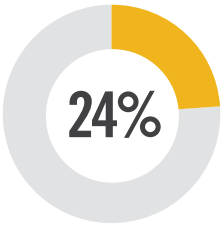
80% Isolate and shut down offending systems and accounts, recover encrypted files from backups, mitigate the initial attack vector if possible.



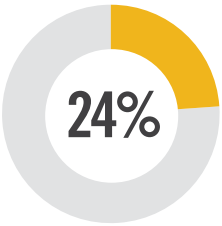
Proactively shut down core systems to prevent spread



Contact cybersecurity technology vendor



Attempt to decrypt files ourselves



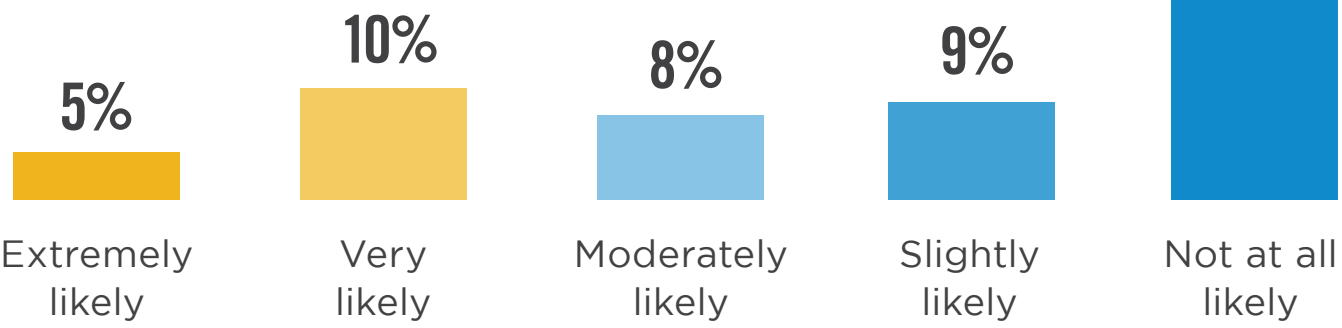
Immediately call law enforcement

Engage a third-party incident response service 24% | Contact cyber insurance provider 24% | Notify customers 20% | Pay the ransom 6% | Attempt to negotiate with the attackers 6% | Other 2%

NO PAYMENT

When asked how likely organizations are to make ransom payments, the vast majority of survey respondents say they will not pay (68%).

How likely is your organization willing to pay for recovering data affected from a ransomware attack?



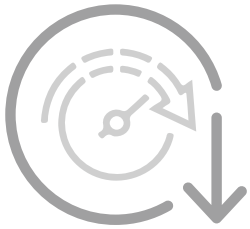
RANSOMWARE DEFENSE

The biggest motivator for improving their organization's ransomware defense is the protection of sensitive business data against attack (73%), tied with preventing system downtime (73%). This is followed by mitigating the financial cost generated by ransomware attacks (66%).

What is your organization's primary driver for improving ransomware defense?

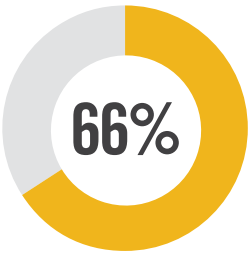
73%

Protecting confidential data related to the business and clients

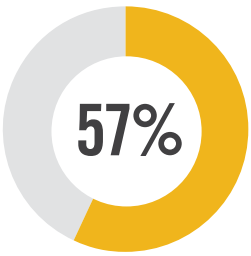


73%

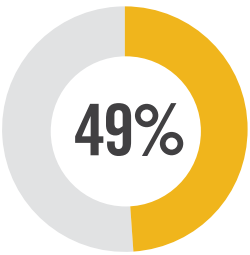
Saving the organization from potential downtime



Mitigating the financial costs arising from ransomware attacks



Protecting the reputation of the brand



Staying a step ahead of emerging threats

Other 1%

EFFECTIVE PREVENTION

When asked about the most effective security solutions to combat malware/ransomware, security professionals rank anti-malware/antivirus/endpoint security solutions highest at 75%. This is closely followed by user awareness and training as the next most effective strategy to prevent and block ransomware (70%).

What security solution(s) would you say is (are) most effective to prevent and block malware/ransomware?

75%

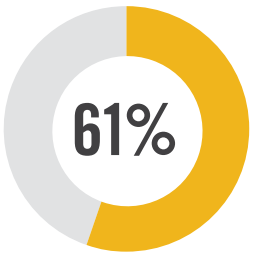
Anti-malware/ antivirus/endpoint security solution

70%

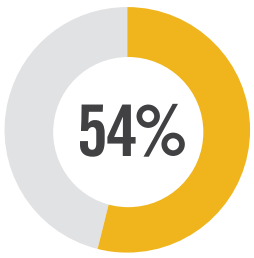
User awareness and training

63%

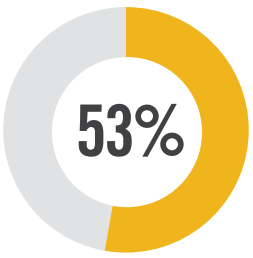
Updating/patching operating systems and software with latest versions



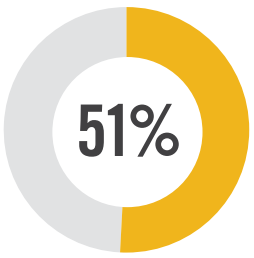
Email and web gateway



Endpoint Detection and Response (EDR)



Network IDS/ traffic monitoring



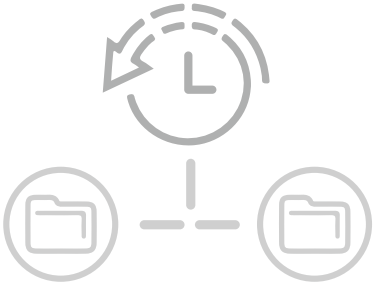
Infrastructure security monitoring

Spam filters 50% | Internal access controls and authentication 50% | Behavior-based/machine learning endpoint protection 45% | File monitoring 38% | Application whitelisting 36% | Sandbox 35% | User monitoring 34% | Other 4%

EFFECTIVE RESPONSE

Cybersecurity professionals continue to view data backup and recovery (86%) as by far the most effective solution to respond to a successful ransomware attack. This way, organizations can often restore critical data without having to pay out ransom to cybercriminals.

What security solutions would you say are the most effective to respond to malware/ransomware?

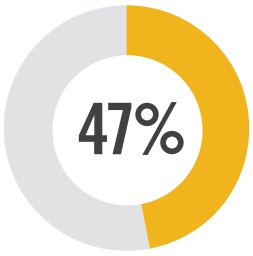


86%

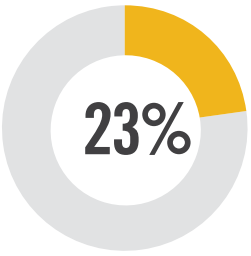
Data backup and recovery response

77%

Threat intelligence



Behavioral analytics

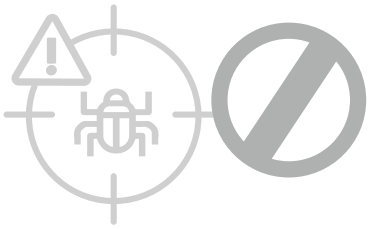


Cyber insurance

ENDPOINT SECURITY

When asked about the most effective endpoint security capabilities to protect against malware, most respondents agree that detecting and blocking malicious behavior (64%), and blocking ransomware and other attacks pre-execution (60%) rank as the most effective endpoint security capabilities.

What do you think is the most valuable endpoint security technology to have?

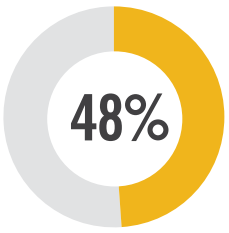


64%

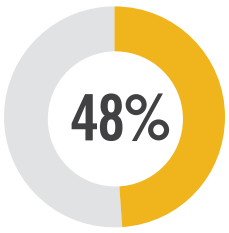
Detect and block at the first sign of malicious behavior (i.e., encryption)

60%

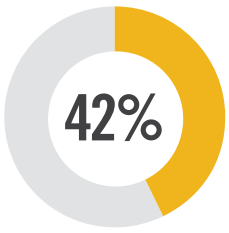
Block ransomware and others at pre-execution to stem the spread



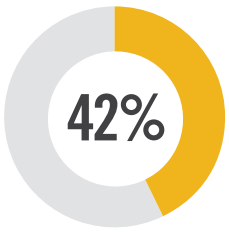
Non-signature based detection and prevention technologies (i.e., machine learning and behavior-based)



Advanced file analysis (i.e., nextgen antivirus tools)



Built-in web security preventing access to phishing, fraudulent or exploit-hosting sites



Fileless/exploit prevention through real-time behavior analysis

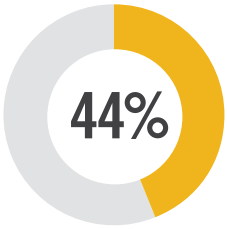
Automatic mitigation including the ability to roll back changes 38% | File-based detection - signature-based traditional antivirus 38% | Endpoint integrated sandbox 36% | Built-in anti-exploit 28% | Other 3%

OBSTACLES TO DEFENSE

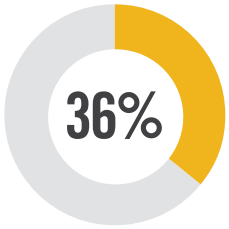
The three biggest obstacles standing in the way of stronger malware and ransomware defense are all about resources and staying current on the latest exploits: lack of budget (50%), dealing with evolving sophistication of attacks (44%), and lack of expert staff/human resources (36%).

What do you believe to be your organization's biggest obstacles to improving malware/ransomware defense?

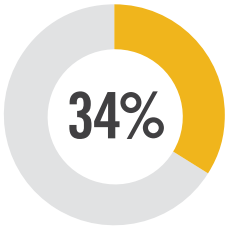
50%
Lack of budget



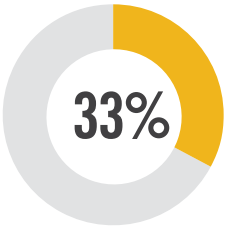
Evolving sophistication of attacks



Lack of human resources



Poor user awareness



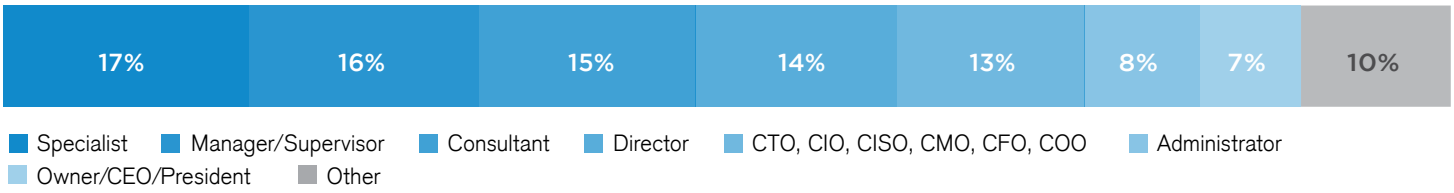
Growing proliferation of attacks

Uncertainty what security solution to use 25% | Lack of executive sponsorship 22% | Our partners' lack of preparedness or response 15% | Other 6%

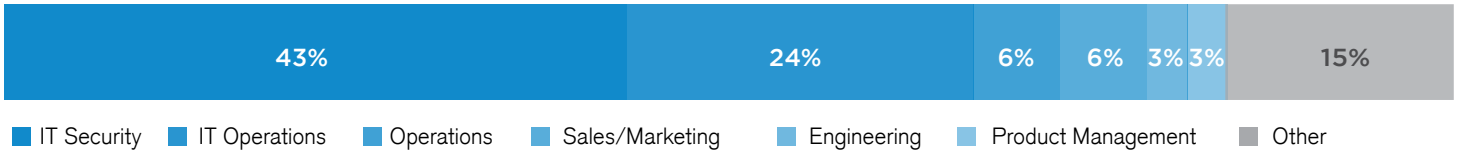
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of cybersecurity professionals to gain more insight into the latest trends, key challenges and solutions for malware and ransomware security. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

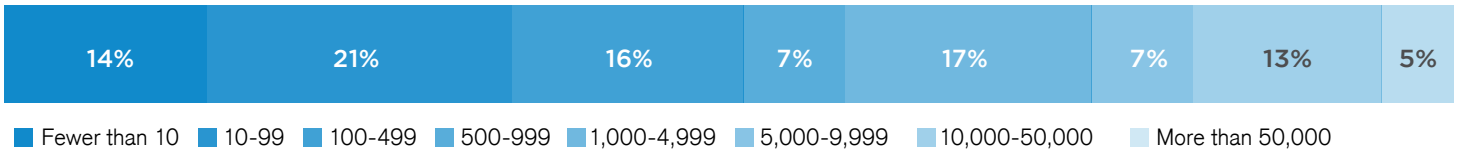
CAREER LEVEL



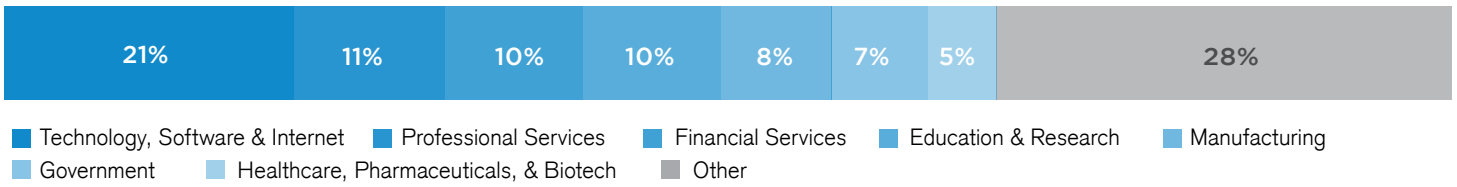
DEPARTMENT



COMPANY SIZE



INDUSTRY



Core Security provides leading-edge cyber threat prevention and identity governance solutions to help you prevent, detect, test, and monitor risk in your business.

www.coresecurity.com