Orange
Cyberdefense

Beating ransomware

A comprehensive guide to tackling the cyber extortion threat

Executive summary

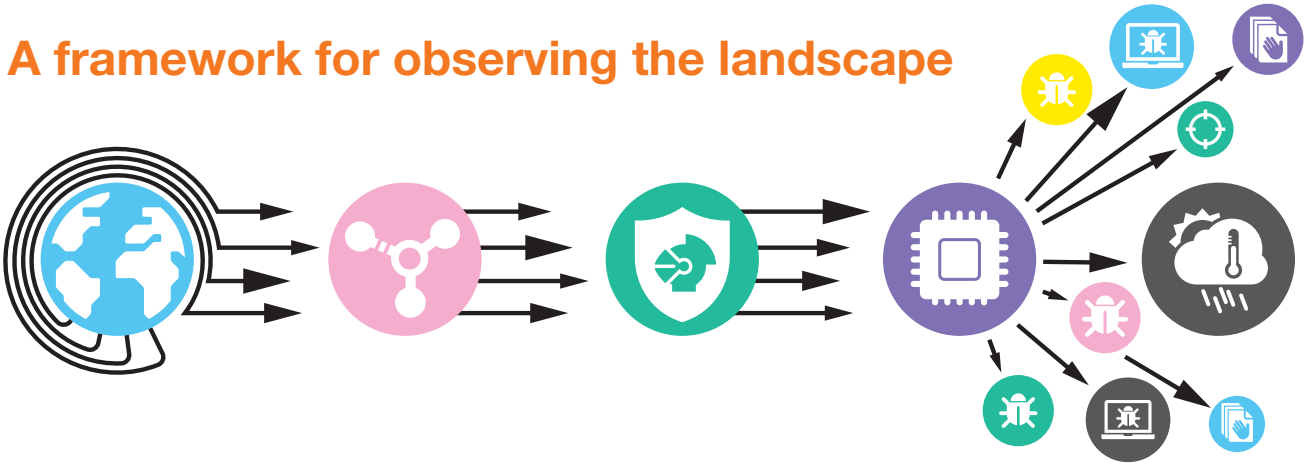
Ransomware has come to dominate the current security discourse, appearing ever more frequently in security news reports. And those are only the cases we hear about. Businesses of all sizes and kinds are being held ransom in the modern "double extortion" variant of this insidious crime.

The purpose of this report is to provide technical guidance to CISOs and security managers concerned with the threat of cyber extortion. However, it is essential to note that cyber extortion is not actually a "technology" problem, and therefore technical controls alone will ultimately not fully resolve it.

Cyber extortion is a crime like any other, and a crime first and foremost. As such, it emerges from a specific political, economic, and cultural context. Its growth is fueled primarily by social and cultural drivers, and its particular shape is the convergence of technology and economics. It should be clear that our response to this scourge needs to be as layered and multifaceted as the diverse factors that converged to create it in the first place.

However, cyber extortion persists because we have built and continue building a technology landscape that can't be realistically protected in the face of such overwhelming systemic forces. Addressing the challenges in the technology landscape under your control is therefore the focus of this report.

A framework for observing the landscape



Ransomware: a crime by any other name

To counter the ransomware threat, we need to first understand what ransomware is. While the term "ransomware" is generally understood, it falls short of wholly capturing a complex and evolving issue. Let's take a moment to clarify the common terms so that we may propose a definition that better suits our needs:

Malware: any software that has been designed to operate in a malicious, undesirable manner, without the informed consent of the computer owner or user.

Ransom: a consideration paid or demanded for the release of someone or something from captivity[1].

Ransomware: malware that holds the data of a computer user for ransom.

Big game hunting: a targeted ransomware operation that involves infiltrating large corporate or government networks that will be significant and lucrative.

Extortion: is the act or practice of wresting anything from a person by force, duress, menace, authority[2].

Double extortion: an evolution of the ransomware business model in which hackers first extract large amounts of sensitive data before encrypting a victim's data. They then threaten to publish the data unless the victim pays ransom demands. This puts extra pressure on organizations to pay up.

These definitions all accurately describe the evolution of the criminal business model and the challenges we have faced thus far. However, the terms malware, ransomware, double extortion, data and even ransom have not remained consistent during the evolution of this crime.

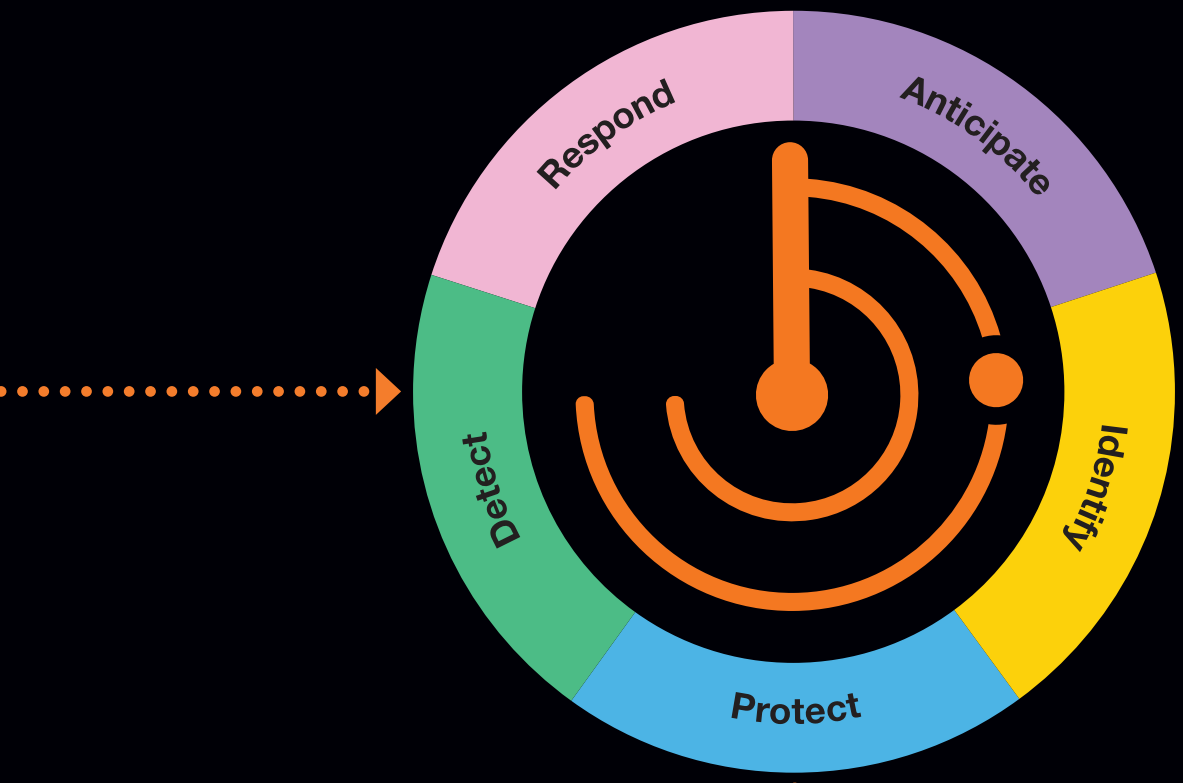
What does appear to be consistent in this form of crime is the notion of extortion. At the heart of the ransomware crimewave is the basic idea that if you take something unique and precious from someone, they'll pay to have it back. If you discover someone's secret, they'll pay you to keep it secret. If they consume all your bandwidth, you'll pay them to stop. The microcosmic market of one seller and one desperate buyer involved in these acts of extortion drives immense profits for the criminal.

The term double extortion describes a specific form of ransomware attack but it doesn't make for a good general definition. To capture the history, the current form, and potential future of this insidious form of cybercrime, we therefore propose to use the term "**cyber extortion**" for this report.

Cybersecurity framework

The US National Institute of Science and Technology (NIST) has developed a Cybersecurity Framework[3] as guidance for organizations to better manage and reduce their cybersecurity risk. The NIST framework is widely referenced and applied. It describes five different functions: identify, protect, detect, respond and recover.

At Orange Cyberdefense we have adopted a modified version of the NIST framework that maps to our own capabilities. We have also introduced a function that is not sufficiently clear in the NIST model, namely "Anticipate". We will use this extended version of the NIST framework to help you structure and evaluate your response to the cyber extortion threat. As such our report is structured around the following five functions groups.



More than a technology problem

Crime is the dominant factor in all cybercrime. If we want to understand the cybercrime problem, we need to recognize that factors like innovation in crime business models, monetization, and markets by criminals have a significant impact.

We believe that cybercrime emerges from a complex system of contributing factors that interact in similar ways to climate and the weather. By identifying and tracking the systemic elements that constitute the cyber threat climate, we can begin to understand and predict the specific threats we experience daily, and therefore plan and prepare for them.

We propose that four layers of systemic force create the issue of cybercrime as we experience it today:

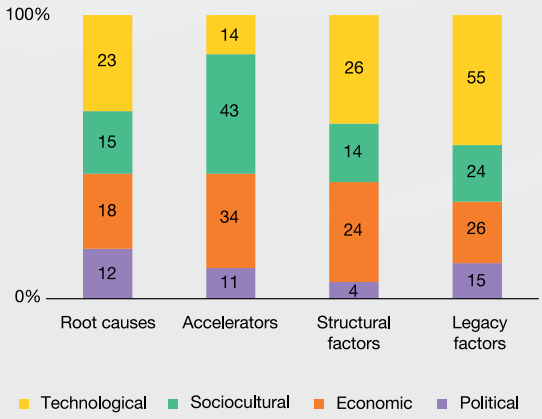
1. **Root causes of the cybercrime problem.** Naturally, this creates a "chicken and egg" dilemma, but essentially, we try to answer the questions: why is there hacking, why is there crime, and why is there cybercrime?

2. **Catalysts that exacerbate the problem of cybercrime.** These factors make the root causes identified in the first layer worse. Here we are trying to answer why cybercrime has become such a significant problem and why does it continue to grow?

3. **Shapers that give the problem of cybercrime the specific "shape" it has today.** The previous two layers help us to understand why cybercrime is a growing problem. This layer helps us understand why it takes the specific forms we experience most often. In the context of cyber extortion we're asking: why is extortion the dominant form of cybercrime today, and why are attackers using the techniques they do?

4. **Legacy factors that consistently serve to perpetuate the problems of hacking and cybercrime.** Unlike the catalysts and shapers, these legacy factors don't have a perceptible impact on the size or the shape of the problem. Instead, they are characteristics of the landscape that act as "blockers" in our battle by making the problems very difficult to address.

If we assign weights to the various systemic factors, we can develop a sense of which elements of the overall threat landscape have the most bearing on the multiple layers of our model: political, economic, sociocultural, or technological. The results of our analysis can be seen below:



Even a casual glance at the chart left suggests that the most prominent contributors to the cyber extortion problem that we experience today are **sociocultural catalysts** and **technological legacy factors.**

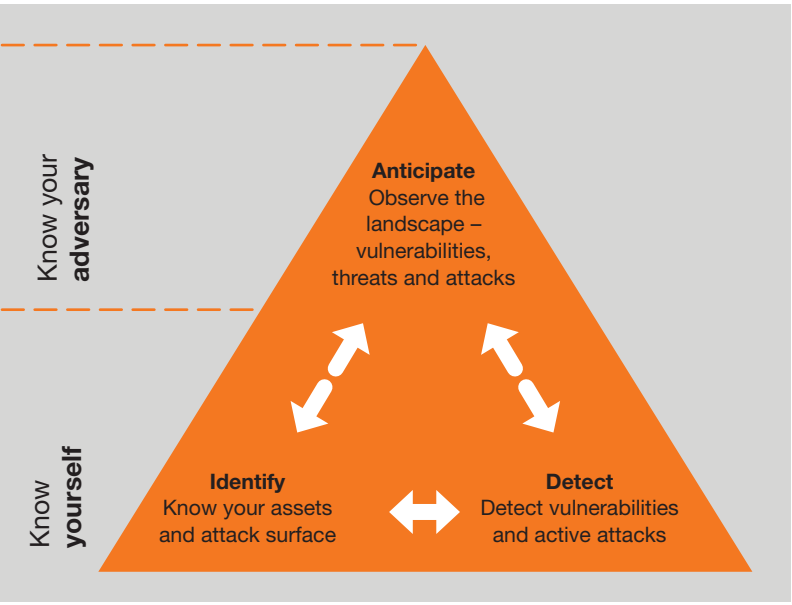
These two elements of our model broadly pit the real-life context of the criminal against the deep-rooted security debt that has accumulated in our technology stacks as we have rushed over the past three decades towards an "everything digital, everything online" society.

Anticipate

Anticipate the latest cyber threats and minimize digital risk

Although the current trend amongst high-profile cyber extortion groups is to target successful organizations for massive ransomware payments, almost anyone can become a victim and should be prepared for that eventuality. By anticipating that you might be a victim and understanding what forms an attack might take, you can then assess your readiness and prepare accordingly.

It is essential to have a real-time perception of the changing threat landscape, including vulnerabilities, tools, techniques, and other relevant factors. This will help you adjust your tactics and apply your resources to have the most impact.



Your preparation should include keeping abreast of developments and new techniques being used by attackers to breach networks. By taking an intelligence-led approach to security, you can better understand the current climate regarding attacker tactics, techniques and procedures (TTPs), and what steps can be taken to counter them. This allows you to focus your resources on the areas that will provide the most reward in terms of detection and prevention capabilities.

Vulnerability management and threat detection, in particular, need to be led by relevant intelligence.

Scanning, security information and event management (SIEM), endpoint detection and response (EDR) and intrusion detection system (IDS) tools will no doubt be updated at some point to test for relevant indicators of compromise (assuming you have sufficient telemetry). However, you'll want to assume that the attacker is already active in your environment. You will need to understand how to search for indicators of compromise after the fact. Such indicators need to be broader than just the traditional markers like file hashes and IP addresses provided to you in threat intelligence feeds. Attackers are clever at hiding in normal traffic and behaviors.

Finding them requires a keen understanding of what they do and how they do it. Changes in attacker behaviour, or new intelligence about attacker behaviour should trigger a new hunt for breadcrumbs across the telemetry, data and systems you have at your disposal.

According to cybersecurityventures.com, cybercrime costs have risen worldwide from $3 trillion in 2016 to $6 trillion this year. In 2025, it is expected to reach $10,5 trillion.

The commoditization of ransomware 5-6 years back has further increased the "opportunity" to make money.

Prepare your people

Ongoing user awareness training can also benefit from ongoing intelligence. Put training and testing based on real and current threats in place to provide your employees with the tools they need to identify attempted phishing emails, social engineering attempts or other markers of a possible attack.

Document your incident response plan

Another key component is to establish a documented incident response process that all employees are aware of and know how to initiate. It should be based on an appreciation of other victims' experiences and tested against real-world case studies, using tabletop exercises and targeted red team exercises, for example. You may also want to keep hard copies of these processes readily available in case they are compromised in an attack. These processes must be regularly tested and updated to ensure they stay relevant to the business and address any new threats or risks.

Plan with intelligence

In the worst-case scenario, you may find yourself faced with a compromise, with your data encrypted and ransomed. Even in this scenario, you can benefit from the insights gleaned from intelligence. Security analysts constantly study ransomware negotiations to compare various approaches, assess the effectiveness of negotiators, and predict the probable trajectories of a negotiation.

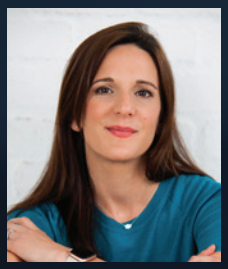
You will be able to serve your company much better in the event of a compromise if you have assessed such intelligence and considered it in preparing for the worst possible eventuality. Your job as a security leader today has as much to do with managing these kinds of disasters as it does managing patches and passwords. Planning and preparation will serve you enormously.

Finally, intelligence can inform your decisions regarding cyber insurance. We strongly advocate against paying ransoms (as we will articulate later), but one must recognize that there are cases where the business may have no other options. Whether to pay the ransom, or pay for a recovery process, funds from an insurance policy may play a vital role. Your decisions regarding the size and form of a policy, as well as your choices of provider and assessment of the policy itself, will be well served by a solid and current understanding of the threat landscape and its implications.

A solid backup strategy can be vital in recovering from a ransomware attack without paying the ransom. These backups, or copies of them, should be kept offline to protect them from being encrypted or deleted. It is also crucial to regularly test the backups to ensure they are working and that systems can be restored using them.

The key to successful security awareness education

We asked Anna Collard, SVP Content Strategy & Evangelist at KnowBe4 AFRICA, to describe the keys points involved in preparing a successful user security awareness program.



1. Get active executive involvement

You need executive involvement that goes way beyond sponsorship or budget approval for the campaign. Your executives need to be the face of your campaign, because people look at what their leaders are doing. Get a one-minute video clip of your CxO sharing why security is important to the business and them personally.

2. You can't manage what you can't measure

Create a baseline view of your current status by running a proficiency or security culture assessment and track it every 12 months. This will allow you to showcase improvements. Phish prone percentage (PPP) can help as a tracking metric but can be manipulated by changing phish sophistication levels, so this needs to be reported in context.

3. Avoid cognitive overload

Focus on two or three key behaviors and/or messages at a time and repeat these throughout your campaign. Don't throw the whole security book at your people, as the danger is that nothing will stick.

4. Don't do it alone

Work with your marketing, internal communications, HR and compliance teams, amongst others. SANS just published a report saying that at least 2.5 full time employees (FTE) need to be dedicated to a successful security culture program.[4]

5. Make it beautiful

This is the visible face of your department, so make sure your communications are beautiful, simple and impactful. Choose content that is personally relevant and interesting to people (protect your kids, your home etc.).

6. Use a carrot and stick

Combine positive with negative incentives: reward desired behavior such as public shoutouts for someone reporting a nasty phish, or bonus payments for anyone not falling for a simulated phish in a certain timeframe. Negative incentives can include automatic remedial training for clickers, and line manager follow-ups for non-participation.

7. Perform relevant tests

Combine training with frequent and random phish simulations. Doing quarterly phishing is not enough. Everyone in the company should get a randomly-assigned phish every week. This gamifies the experience as every email needs to be scrutinized.

8. Be human

Emotions are powerful engagement techniques, so use them in your content. Tell stories and use humor.

Anticipate checklist

Check	Control	Impact
	Have I considered my cyber insurance policies in light of contemporary intelligence about recent compromises in my area of operations?	High
	Am I in a position to learn about changes in cybercrime practice and adapt my threat detection and vulnerability management strategies and tactics accordingly?	High
	Am I aware of the most common vulnerabilities and misconfigurations being deployed by extortion operators (e.g. credentials stuffing against RDP and VPNs), so that I can scan my environment for these issues specifically?	High
	Am I in a position to understand, learn from, and adapt to the experiences of recent victims in my sector?	High
	Are my IT staff and regular employees properly informed about extortion tactics and techniques in order to spot the signs of an attack or compromise in progress?	Medium
	Do I fully understand the tactics, tools and procedures used by contemporary extortion groups?	Medium
	Have I conducted table-top and technical exercises based on understanding how contemporary attacks and extortions play out?	Medium
	Do I have a good understanding of how an extortion negotiation is likely to play out, and have I adapted my own counterstrategy accordingly?	Low
	Do I know what cyber extortion groups are operating in my country and industry, and targeting businesses of my size?	Low

Identify

Identify your critical assets, data and vulnerabilities to prepare your security strategy

Manage the vulnerabilities attackers will exploit

Your first step is managing the most likely entry points for an attacker. These include compromising an end-user via phishing or social engineering, password spraying, or brute force techniques against exposed RDP servers. Exploiting vulnerable systems allows attackers to get a foothold in a network or move laterally once inside.

Even if a vulnerability isn't the initial point of access, attackers frequently use local privilege escalation vulnerabilities (PrivEsc). They facilitate credential grabbing, malware infection, command & control, lateral movement, service manipulation and ultimately encryption. **Don't underestimate these "local" vulnerabilities**. Tackling them can play a major part in managing the eventual impact of an initial compromise.

Vulnerability management program

Set up a robust vulnerability management program to identify and patch vulnerable systems. This should cover all internet-facing systems as well as internal devices. It is imperative to include security solutions such as firewalls, RDP and especially VPNs in this program.

Establishing and maintaining an effective vulnerability management program is something most organizations still find to be a painful and difficult undertaking – especially when considering what can seem to be a flood of new vulnerability disclosures.

The first step in setting up a vulnerability management program is to perform an asset discovery exercise. This will identify the systems deployed in your environment and allow you to maintain an accurate inventory. Depending on your environment, hardware can be as important here as software.

What our responders see

Thomas Eeles, Cyber Security Incident Response Team (CSIRT) manager in the UK, says that the technical control failures he sees most consistently at the incidents his team responds to include:

- **Poor user account control**, including weak passwords, password reuse and excessive account privileges.
- Poor Remote Desktop **(RDP)** control. RDP servers are too often exposed to the Internet, and protected only by user accounts and (weak) password.
- Lack of **multi-factor authentication** leaves customers exposed to credential stuffing attacks

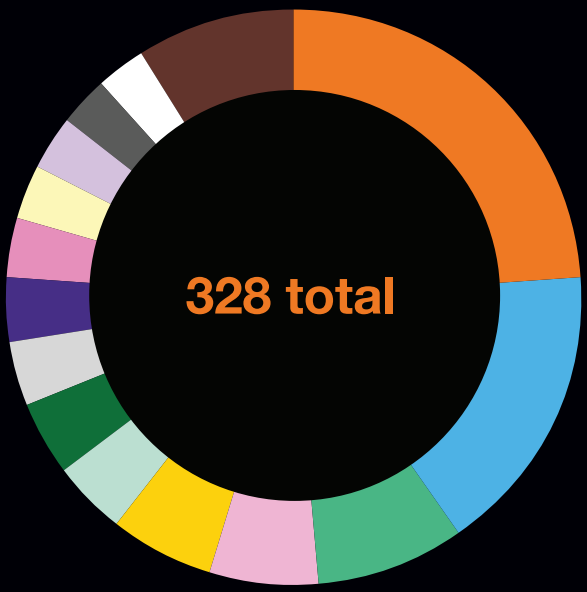
Thomas emphasises that most attacks he responds to are perpetrated by criminal gangs with no advanced attack techniques. **"The threat is persistent, but usually not advanced".**

Just in case:

You can find your country's emergency CSIRT hotline on

orangecyberdefense.com/emergency/

Don’t forget the hardware



	%
Continuous vulnerability management	24.09
Inventory and control of software assets	16.46
Inventory and control of hardware assets	8.23
Account monitoring and control	6.10
Maintenance, monitoring and analysis of audit logs	5.79
Limitation and control of network ports, protocols and services	4.27
Application software security	3.96
Controlled access based on the need to know	3.66
Incident response and management	3.66
Secure configuration for hardware and software on mobile devices, laptops and workstations	3.35
Boundary defense	3.05
Malware defenses	3.05
Data protection	2.74
Email and web browser protections	2.74
Other	8.84

Summary of recommendations made in our World Watch intelligence advisories for Q1 2021

Most of the recommendations emerging from the World Watch security intelligence service we provide fall under the basic CIS controls of inventory and vulnerability management. Moreover, hardware inventory has become more important, growing from 5.9% to 8.3% of all recommendations made during the first quarter of 2021.

Vulnerability scanning

Once you have identified these systems, you should assess them to determine the actual risk level for each device or group of devices based on their criticality to the business. This exercise can then be used to prioritize devices when it comes to deploying patches to them.

The next step is to regularly run scheduled vulnerability scans against the estate to identify vulnerable assets. The output from these scans should be a report which should identify the highest-risk devices based on their own criticality rating alongside the risk posed by the vulnerabilities present. **The risk evaluation needs to consider the value and exposure of the asset, the assigned seriousness of the vulnerability, the age of the available patch and any intelligence about the existence or use of an exploit.** This should then be used to prioritize the remediation of devices by deploying patches automatically or manually as appropriate.

There are two approaches to vulnerability scanning, and both need to have a place in your vulnerability management program:

1. Regularly scan and patch to reduce your overall level of risk. Regular vulnerability scanning is analogous to brushing your teeth. You need to perform it regularly and diligently, just to keep abreast of the threat. Of course, the scanning is only as useful as the triage, mitigation, and measuring efforts that emerge from it, but done properly, vulnerability scanning and patching or remediation will put you way ahead of the curve. Regular scanning, even if performed meticulously, is only the beginning though. The threat changes, and we need to respond continuously.

2. Ad-hoc searches for systems with specific vulnerabilities or attributes that are being exploited by attackers. There are thousands of vulnerabilities disclosed each month. For example, between 2018 and 2020 the US National Vulnerability Database officially recorded an average of 1,524 vulnerabilities a month, across 6,744 vendors. And there are likely to be many more we don't know about. Chances are, you won't be able to address them all as quickly as you'd like. But only a fraction of vulnerabilities ever actually get exploited "in the wild". A report from Kenna Security suggested that only 2.6% of 18,000 tracked vulnerabilities were exploited in 2019[5].

With the right intelligence about the severity of specific vulnerabilities, you can adjust patching priorities appropriately. Intelligence has two facets: not only do we need to know what kind of systems to worry about, we also need to identify those systems within our environments. The ability to rapidly perform scans or (preferably) searches across the IT inventory to identify the systems or services most vulnerable to current attack vectors, is the second characteristic of a successful vulnerability management program.

Penetration testing

You should carry out regular penetration testing alongside your vulnerability management program on internal, internet and cloud environments. This will help identify any other weaknesses besides vulnerabilities, such as misconfigurations, and test that patches are being successfully deployed.

Penetration testing will also serve to highlight other ways an organization is vulnerable to attack, such as password spraying, or brute force attacks on systems or services. Internal testing will identify how easy it is for an attacker to elevate privileges and move laterally through your environment. These play a critical role in a manually-operated extortion attack and any measures that a penetration test can identify to restrict or prevent this are crucial and should be acted upon.

Practice how they'll play

It's essential that at least some of your testing is designed to mimic the techniques of contemporary cyber criminals. This includes scoping the tests to incentivize the same aggressive technical and social engineering techniques contemporary attackers are actually using. It's no good testing for weaknesses you already know about. **Find and engage with testers you can trust to truly exercise your security technologies and processes using real-world, intelligence-led techniques.**

An emerging approach to penetration testing is called "purple teaming". Derived from the traditional labels of "red hat" and "blue hat", this approach seeks to actively test detection and response capabilities (as well just protection mechanisms) and deliberately involves your security and operations team in the exercise. In a purple team exercise, your security teams are invited to participate in the process and given the opportunity to assess and refine their capabilities with guidance from a battle-tested adversary.

Identify checklist

Check	Control	Impact
	Do I have a comprehensive view of my IT assets, particularly my internet footprint, so that all internet-facing systems are considered in my vulnerability management program?	High
	Am I regularly checking for internet-facing systems that are commonly used in attacks, particularly RDP and VPN, so that they can be included in penetration testing and vulnerability scanning?	High
	Do I have effective vulnerability and patch management that ensures relevant security patches are being identified, triaged, and remediated within an appropriate time?	High
	Does my business engage regular penetration tests or red team exercises that emulate the tools and tactics that actual cyber criminals are deploying, and can testing proceed without excessive limitations or constraints?	High
	Does my vulnerability management consider all internet-facing systems, including those that are hosted, in the cloud, in reserve or apparently deprecated?	High
	Am I identifying and patching local privilege escalation vulnerabilities, especially those commonly used by extortion operators?	High
	Am I routinely checking for issues with weak passwords and password reuse, which cyber criminals commonly exploit?	High
	Do I have access to intelligence that informs me when the risk rating for a system, service or vulnerability needs to be re-rated?	Medium
	Can I perform ad-hoc scans or searches to identify systems or services that may have become an attacker vector for criminals since the last time I scanned?	Medium
	Are my SOC and response teams involved in penetration testing exercises so that they can acquire proper “battlefield” experience and practice identifying and responding to a skilled and determined adversary?	Medium
	Am I certain that my vulnerability management program has sufficient scope and covers all the systems an attacker might target, including remote worker PCs, Linux, OSX, appliances, and connected hardware, wherever they may be connected?	Medium

Protect and detect

Protect your organization with the right technology and skills and detect cyber attacks through analysis of alerts and behaviors

Endpoint protection, detection and response

The most obvious place to detect and disrupt malware and ransom activities is on the endpoint. The growing attack-surface presented by a desktop, its value in terms of data and as a foothold, and mistakes often made by users have made the endpoint an increasingly popular target.

This has dramatically altered the network security paradigm. Where once it was sufficient to protect only the perimeter of a corporate network, this outdated approach is now no longer enough. Instead, **there must be a new, comprehensive, and ongoing focus on endpoint security**. Endpoint detection typically takes the form of anti-virus or endpoint protection, detection and response (EDP/R), also known as “next generation” anti-virus.

The value proposition of endpoint solutions is that they can detect the signatures of malicious files or processes, or even suspicious traffic or other behaviors. They then block the processes from executing and quarantine the suspicious files. The basics of how crypto ransomware behaves is well known; the malware somehow gets onto a system, encrypts certain filetypes and then displays a ransom note. The targeted filetypes, encryption method and ransom notes may vary, but security vendors generally know what kind of behaviors can be observed during a ransomware attack in order to detect them.

Real-time behavior

Endpoint protection now needs to know how to pick up real-time malicious behavior on an endpoint, instead of just known malicious signatures and heuristics on the file system. This involves the continuous collection and processing of significant amounts of data from an endpoint.

Furthermore, **77%[6] of successful attacks used fileless malware** that older endpoint security tools struggled to prevent. Since detection of fileless malware and similar types of advanced attacks cannot be done with only static rules or signatures, **you need the ability for behavioral anomaly detection on the endpoint.**

This behavior needs to be analyzed and correlated across other endpoints to separate the false positives from the real incidents. Without the right tools and competencies, this can take a very long time. Once the investigation phase is complete, any critical incident will most likely also require rapid response actions. If the time from compromise to detection and remediation takes too long, it greatly increases costs and damage that could have been avoided.

77% **of successful attacks used fileless malware[6]**

Choose the right EDR

The choice of endpoint detection & response (EDR) solution therefore plays a significant role in protecting your endpoint clients and servers from ransomware and other malware.

There is a whole myriad of EDR solutions available, making it difficult to select the right one. **Ideally a solution will use multiple detection techniques,** including signature-based, static IOCs and behavioral analysis capabilities. As our study shows, next-generation offerings that have local "intelligence" in the form of models (either machine-learning trained or manually crafted) for decision making appear to perform better in the face of modern threats. This also adds the ability for the agent to act quickly and autonomously without being requiring continuous internet connectivity.

The solution should be cloud-based, allowing continuous monitoring and centralized collection of activity data, along with the ability to perform remote remediation actions – whether the endpoint is on the corporate network or outside of the office. In addition, the endpoint agent does not have to maintain a local database of all known IOCs but can query the cloud system for analysis of objects that it is unable to classify.

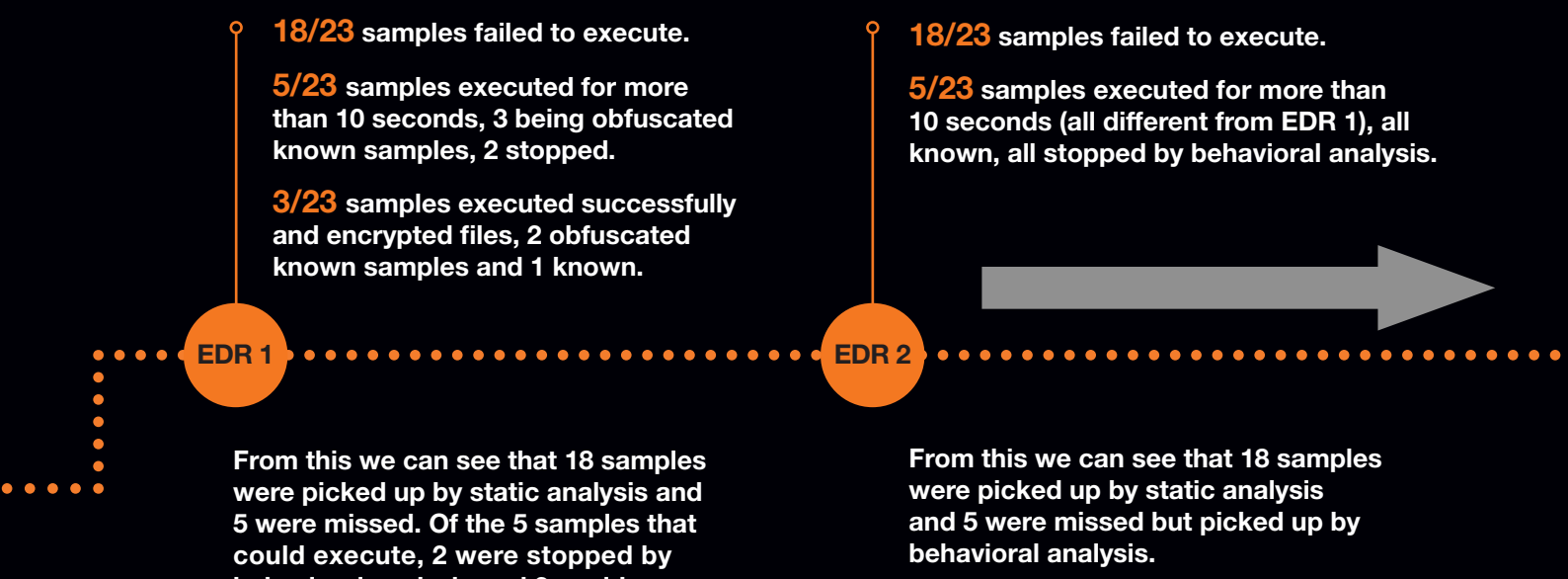
EDR success lies in the details of the implementation

You should also **factor in the complexity of EDR solution deployments**. It is comforting to believe they are fire and forget solutions, but this is often not the case. You need to determine whether you have the in-house capabilities and workload availability to effectively deploy, manage and tune the solution. If not, you should consider using a service provider to ensure optimum protection.

Whichever solution is chosen it needs to have coverage for all the major operating systems in use in your environment. We would also recommend going with a single solution that provides the benefits of standardized reporting, easier data correlation, and one interface from which to manage alerts.

Most EDR work. But some work better than others.

In an experiment performed by our Security Research Center, EDR solutions were chosen and configured using the suggested industry-standard configurations and agents were installed in an up-to-date Windows 10 machine. Samples were run and the outcome evaluated by rThreat, an attack emulation solution. We could track if the file was executed, for how long, and if it was stopped. We tested both known and unknown threats that follow TTP standards, are mapped to the MITRE ATT&CK framework, and tested across the entire kill chain, to reflect authentic APT practices.



Dominic White is the Ethical Hacking Director at Orange Cyberdefense.

"There's a weird fetish in infosec to 'do the basics first'. They tend to focus on prevention, with detection saved for when you have an expensive blue team and SOC. But what offensive work will teach you is that many of the things people think of as preventative controls are often only detective controls. Take AV, it's cheap to bypass in the short term, but sometimes a midday update could unmask part of your toolkit and trigger an alert[7]."

Our results for the 23 samples demonstrated the different approaches EDR solutions have, as they did not act in the same way and do not have the same signature databases, which did not come as a surprise. Of course, it is difficult to compare EDR solutions as there are so many factors in play and so many configuration options.

22/23 samples failed to execute.

1/23 samples ran for more than 10 seconds, obfuscated known sample, stopped.

EDR 3

From this we can see that 22 samples were picked up by static analysis and the one that got away was detected by behavioral analysis.

23/23 samples ran for more than 10 seconds, they were terminated by the EDR.

EDR 4

From this we can see that this EDR configuration allowed for the execution of all the samples, but they were all promptly stopped. This solution seems to rely mostly on behavioral analysis.

The emphasis is on detection and response

The lesson we learn from our penetration testing teams is that all alerts must be investigated even if the solution reports that it cleaned or blocked the activity. Malware and malicious activity should not be present in your environment, so identifying the source or cause of anything detected, even if it is cleaned or blocked, is critical as it could be a precursor to something more sinister.

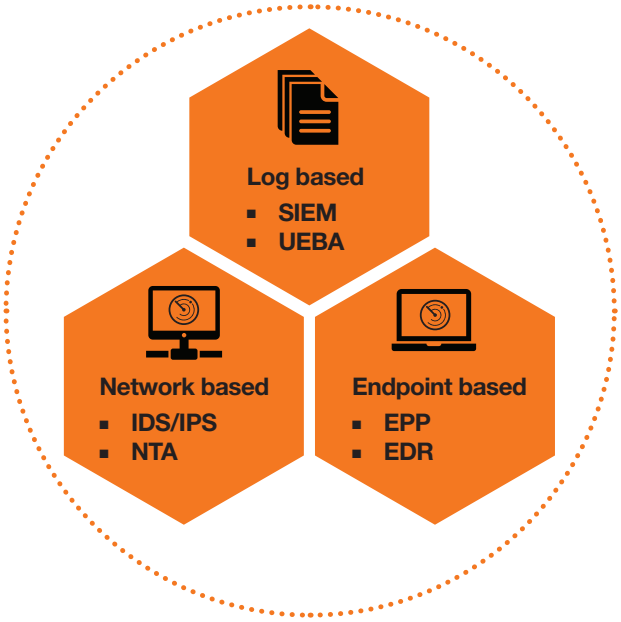
Complement EDR with other forms of detection

Complementary to EDR we would also suggest deploying a network threat detection solution. By analyzing the network traffic at certain choke points in your network, these solutions can identify threats that otherwise may fly under the radar. Using behavioral analysis and AI capabilities can alert organizations to suspicious, malicious, or anomalous traffic flows and patterns. This extra layer of protection can identify threats originating from devices where it has not been possible to deploy an EDR agent or where an attacker has managed to bypass the EDR solution.

Some solutions also can perform automated remediation actions such as terminating connections, quarantining a device or cutting off a subnet to prevent lateral movement. An ideal solution should be deployed in on-premises, virtual and cloud network environments to provide total coverage and protection.

Don't depend on your users to detect malicious content

As already noted, phishing attacks are a key vector for an attacker to gain a foothold in a network. Therefore, a solid email security system must be in place to detect and prevent phishing campaigns and other email-borne threats. An optimal solution would be a vendor's cloud-based service. This provides centralized monitoring and control and allows you to scale as required when the need arises. You also get the benefit from real-time intelligence and protection based on telemetry from the vendor's customer base.



Log based
+ Good hub for collection of logs and alerts
- Not everything is logged

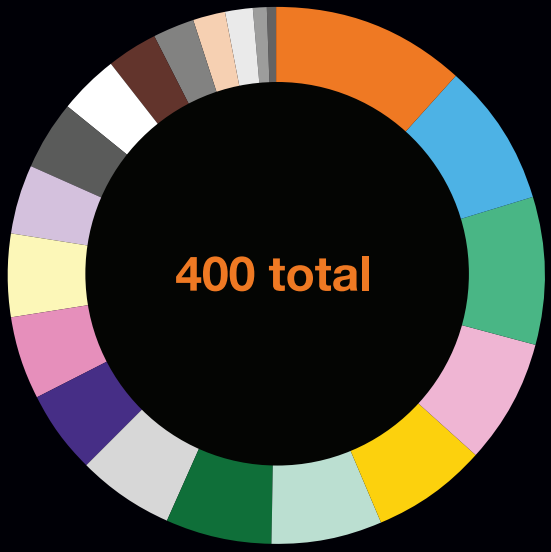
Endpoint based
+ Best detection where you can install an agent
- Threats present on devices without an agent

Network based
+ Detection across all network connected devices
- Activities that happen within an endpoint

Strong authentication, everywhere that matters

You should enable multifactor authentication (MFA)[8] on all internet-facing services, where feasible. **At the very least, MFA should be implemented on email, VPN and exposed RDP services**. This will then restrict other primary attack vectors, namely password spraying and credential stuffing. SMS multifactor authentication mechanisms should only be used as a last resort and should be moved away from at the earliest opportunity. Instead use an app-based or token-based one-time password (OTP) solution, as this removes the risks of a SIM-swapping attack being used to intercept the MFA SMS request.

An analysis of hundreds of incidents handled by our CSIRT in 2020 (about 10% of which were ransomware) shows the distribution of control failures our analysts identified.



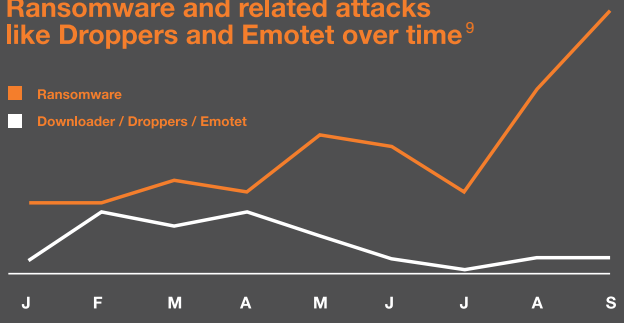
	%
Maintenance, monitoring and analysis of audit logs	11.75
Controlled use of administrative privileges	8.75
Limitation and control of network ports, protocols and services	8.75
Continuous vulnerability management	7.50
Account monitoring and control	7.00
Secure configuration for hardware and software on mobile devices, laptops and workstations	6.75
Implement a security awareness and training program	6.25
Malware defenses	5.75
Application software security	5.25
Incident response and management	5.00
Email and web browser protections	4.75
Controlled access based on the need to know	4.25
Penetration tests and red team exercises	4.25
Data protection	3.50
Boundary defense	3.25
Inventory and control of software assets	2.25
Secure configuration for network devices, such as firewalls, routers and switches	2.00
Data recovery capabilities	1.75
Inventory and control of hardware assets	0.75
Wireless Access Control	0.50

Detection is not passive, it's an active process of engagement

We are tempted to think of detection as a process of looking for big "incidents" where an attacker is caught with their digital hand in the proverbial cookie jar and unceremoniously tossed out.

That's seldom the case, however. Instead, intelligence and detection need to be the starting points for an ongoing process of engagement with attackers. The battles that occur under the process are often little more than skirmishes with subtle indicators of attack or compromise that often produce no clear "victory". Our research suggests that continuously engaging in these skirmishes can produce tangible security results, however.

Ransomware and related attacks like Droppers and Emotet over time[9]



As we reported in our 2021 Security Navigator report, our global CyberSOC operations reported very few confirmed ransomware incidents across our customers. But that doesn't mean there weren't any attacks!

Ransomware is generally the final-stage strategy for a malware infection. It is the last action of a compromise that has already progressed through several other phases of exploitation. Malware operators will extract every possible bit of value from a compromised endpoint before initiating encryption and revealing their presence. **The more successfully we detect malicious activity in the earlier phases and disrupt it, the less likely it is to progress to a ransomware incident.** Our data suggests that an increase in **early-stage detection correlates with a decrease in ransomware detection.**

As we can see in the chart above, we detected and confirmed more ransomware incidents during the first quarter of 2020, which we believe is a function of poor levels of security team responsiveness during the peak of COVID-19. After April 2020, we see a steady increase of detections related to Downloader and Droppers as well as trojans (including Emotet), while at the same time we observe a decrease in confirmed ransomware incidents.

We hypothesize that when security teams turned back to "business as usual" in Q2 of 2020, there were better levels of responsiveness to malware campaigns earlier in the attack cycle and therefore fewer ransomware attacks that succeeded. The significant peak in Downloaders, Droppers and trojans in September is in line with the increased ransomware activity seen in the wild. However, **with improved focus, we seem to have managed to detect and respond to attacks during the early stage of exploitation, and thus confirmed ransomware incidents actually decreased** despite the increase in campaign volumes.

Timeline of an attack as described by the ContiLocker Team

CONTI Recovery Service

Hello, this is ContiLocker Team.

Please, introduce yourself (Company name and position) and we'll provide all necessary information. Sometimes our staff is busy, but we wil reply to you as soon as we possible.

7 days ago

10 Jan — Entering the network

11 Jan — Escalating to the domain admin rights

12 Jan — Lateral movement through the network, data gathering (including IT top tier accesses), identifying protection systems such as Defender and Symantec

13 Jan — Locating eight Veeam backup servers and Nimble Storage containing volumes and some more backups, going through web production systems

13 Jan — Downloading data including databases and file shares

14 Jan — Central Veeam controller is located, all backup engineering is reversed

15 Jan — vCenter is located and the access is gained

16 Jan — Preparation phase, including the planning, sorting data, step-by-step actions

17 Jan — Final phase. Antivirus evaded, Veeam backups are removed and rewritten, backup folder from Nimble Storage is removed

Get the "basics" right

A couple of basic security hygiene practices should be implemented as part of the detect and protect process. While they will not prevent a ransomware attack, they can help to restrict and contain one, thus buying time to detect the attack and eradicate it from your network.

The basics in defeating extortion attacks primarily involve the principle of least privilege and network segmentation, which we cover in detail below. However there are a few other low-hanging fruits you'll want to pick off, including:

1. **Secure VPNs and firewalls.** Many attacks target vulnerabilities in perimeter security technologies. Make you sure you patch them, configure them properly and ensure unique, strong, passwords.
2. **Secure Remote Desktop.** Like perimeter security, remote access is proving to be too rich a target. Take it off the internet, put it behind your VPN, patch and configure it properly, and ensure passwords are strong and unique.
3. **Educate your users.** Employees can be the weakest or strongest link in your security chain. Make sure you equip and motivate them to make good security decisions.
4. **Use a password vault.** Vaults support the use of strong and unique passwords for all systems. It is critical that your administrators are using one, but we would advocate for sponsoring a password vault application for all your employees, even to use for their private accounts.
5. **Upgrade SMB.** Many lateral movement techniques in Microsoft Active Directory environments leverage inherent weakness in the Server Message Block (SMB) protocol. If at all possible you should disable SMBv1 across your entire estate and upgrade to v3 (or v2 if necessary).
6. **Optimize your EDR.** Make sure you have a good solution that is properly deployed and well managed.

Dominic White is the Ethical Hacking Director at Orange Cyberdefense.

"That's a noisy, high false positive alert, so we end up back at needing a blue team to look after the EDR solution data stream. What if instead, we made high quality (i.e. low false positive, low volume) alerting 'the basics'. Something the overworked IT/sec manager could use. Which is partly a justification for why deception techniques can and should make up a bigger portion of sec team work earlier on in the strategy than most people typically put it[10]."

Enforce least privilege

Enforcing least privilege revolves around **only giving a user account or process those privileges which are essential to perform its intended function.** This is not always an easy thing to implement and can often result in pushback from some business areas who see it as disruptive. But it's an essential weapon in your armory.

Feedback from our CSIRT tells us that standard users have been given far too much freedom, access, and privilege on devices and network systems in many incidents they attend. An initial first step is ensuring that a user's standard domain account does not have administrative privileges anywhere. This includes locally on a device or at domain admin level. At the very least, if a user requires some form of administrative access, then a separate account should be provided, which gives them that access only whilst they need it.

Where possible, use a privileged access management (PAM) solution where passwords can be checked out, then checked back in once used and changed. This also extends to a PC's local administrator account. **Every computer's local password should be unique** as this will help prevent lateral movement to other devices if one password is compromised. Microsoft have provided the Local Administrator Password Solution (LAPS) to help manage this.

The principle of least privilege should not just be limited to the standard Active Directory environment, but should also apply on all systems, services and solutions users access. If a user only requires access to one element of a system, or only needs read-only access for example, then they should be granted just those permissions and no more. This can be especially challenging in cloud, multi-cloud or hybrid cloud environments, but it is all the more necessary. In these environments you can configure any human or machine identity with thousands of identity and access management (IAM) permissions to access services potentially containing sensitive information. Due to these complexities, it is very easy to unintentionally provide identities with permissions allowing access to services and resources, which they do not require.

Segment networks as much as possible

Network segmentation uses the principle of least privilege to only allow the network traffic that needs to get to and from a system so it can operate, while preventing all other traffic. This should begin with basic perimeter security, ensuring that only required systems are exposed to the internet and that they are only exposing the required services.

Conversely, **only allow direct outbound access to the internet for systems that absolutely need it**. Many mission-critical servers, for example, do not require any internet access at all, so it is best to simply not allow it. Internal devices should be assessed and grouped together based on their class or risk, these groups should then be placed into their own network enclaves with appropriate security systems at choke points between them. Put rules or controls in place at these choke points to only allow the required traffic inbound and outbound from each enclave – or even down to the individual system level if possible.

If at first you don't deceive

Another area to explore is the concept of deception technologies, which is an emerging element of cybersecurity that is gaining significant traction. **The tactic of deception is particularly effective against human attackers**, as they seek to move laterally through a network. It usually provides solid evidence of an intrusion.

Deception technology uses traps (decoys) and/or lures mixed among and within existing IT resources, which are designed to tempt an attacker to interact with them. As these traps or lures are not "real" and serve no genuine purpose, any interaction with them by an attacker will generate an alert that can be considered concrete.

These traps or lures, often referred to as canaries, can be in the form of specific files, user accounts or even a host system on the network. This can even be extended to processes running on devices, as attackers will try and kill certain processes to disable security products or release files so they can be encrypted. As these processes are quite well-known, fake processes can be created and monitored, so that if they are stopped an alert is generated. While all this can be accomplished internally relatively easily, services do exist to automate the creation and management of these canaries. They make them appear as realistic for your environment as possible, while also catering for more complex scenarios and capabilities.

Deception obviously also needs to be paired with effective detection and response capabilities. Deception alerts are infrequent by design, but of very high fidelity. Accordingly, systems and processes must be put in place to ensure that alerts from deception systems are noted and responded to with appropriate urgency.

Protect your pipes

A recent shift in tactics in cyber extortion, especially when it appears that their ransom demands will not be met, is to launch distributed denial-of-service (DDoS) attacks against a victim. This can be very challenging to an organization already trying to recover from the initial attack and seriously disrupts attempts to put mitigations in place and restore service. The impact of a DDoS attack can be particularly high for organizations in industries such as healthcare or financial services where prolonged downtime can be extremely detrimental.

To reduce the impact of DDoS attacks you should have an initial conversation with your internet service provider to determine what capabilities they have for DDoS mitigation. This will allow you to plan your best course of action. While DDoS protection can be delivered on-premises by placing a solution in front of your network, the protection is limited by the throughput capacity of the device(s) being used. **With attacks increasing to multiple terabits-per-second (Tbps) the solution could soon become obsolete.**

Therefore, **we would recommend the use of a cloud-based provider of DDoS mitigation services**. The first step involved in implementing a solution will require a "learning" period to establish a baseline of what is considered to be normal network traffic. Once this baseline is established, it can help detect abnormal traffic patterns and other methods to identify malicious traffic, such as signatures, packet inspection, and "allow" or "block" lists. Once the solution detects a potential DDoS attack, it can apply mitigations, such as filtering out suspected malicious traffic and applying rate limiting to ensure that business-critical traffic has the bandwidth it requires.

Defending across the kill chain

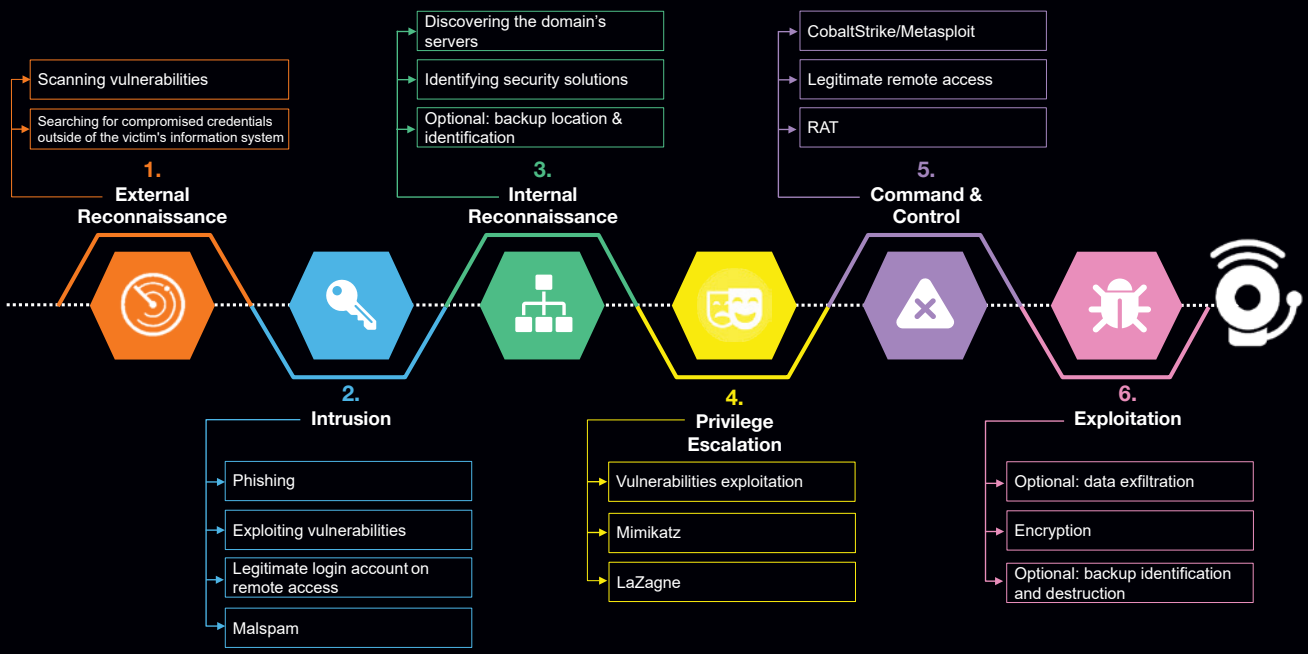
As we emphasized elsewhere in this report, **a confirmed ransomware incident is actually the last stage of a very long and complex chain of events that are described by the so-called cyber "kill chain"**. The actual theft and encryption of the victim's data is typically what we mean when we talk about an attack, leak, compromise or incident, but the attacker has had to do a lot of work to get there. Each of these phases of the kill chain requires specific tools and techniques, leaving a predictable set of breadcrumbs that we can look for to detect an attack in progress.

A mature threat detection strategy takes advantage of this reality by recognizing that there are multiples ways and places to detect an attack in progress. **Detection across the kill chain is not only a best practice, it's an essential practice**. Even the most purpose-built security mechanisms, like EDP/R, can be subverted or bypassed. It's therefore critical to have visibility as broadly across the cyber kill chain as possible.

As we know a chain is only as strong as its weakest link, and so it is with the cyber kill chain. By breaking or disrupting any of the tools or techniques on the kill chain at any point we can prevent an attack from developing to its final phase. **This is a war of several small battles and victory, at any stage of the kill chain, could mean averting a crisis!**

Finally, an understanding of the kill chain presents us with the opportunity to develop a deception strategy. In many of the phases the attacker is somewhat blind with regards to your infrastructure and would find it hard to distinguish between real and fake elements in your environment. This is particularly true in the Internal and External Reconnaissance phases and during lateral movement, where the attacker will be hunting for computers, services, user accounts, and interesting software processes. By scattering fake elements of this kind around your environment you can set a series of traps that could alert you to presence of an attacker at an early stage.

Ransomware: techniques used by cyber-attackers



Protect checklist

Check	Control	Impact
	Have I comprehensively implemented multi-factor authentication (MFA) on all internet-facing systems, including SaaS, RDP and VPN?	High
	Do I have an endpoint security technology that doesn't just depend on signatures, but can also detect and respond to fileless malware and anomalous behaviors, even those that have perhaps not been recorded before?	High
	Have I tackled the low-hanging fruit of ransomware defense: remote access and remote desktop, user education, password quality and management, updated SMB and a solid EDP/R deployment?	High
	Do I have an appropriate endpoint security technology deployed across all the technologies in my environment that may be targeted, including server, workstations, and remote workers?	High
	Have I taken care of the obvious basics? This includes properly protecting all remote access vectors (RDP and VPN), dealing with all vulnerabilities on internet-facing systems and putting suitable filtering in place for inbound email?	High
	Have I limited individual user privileges as much as I possibly can, at very least by ensuring that regular users never have any administrative privileges, and that each computer administrator has a unique account and password?	High
	Given that not all EDR and AV are equal, have I invested enough in an endpoint security technology that weighs up sufficiently against contemporary threat vectors?	Medium
	Have I comprehended that EDP/R and AV are as much about detection as prevention, and have I organized my team and processes to respond with sufficient suspicion and aggression to any endpoint alert?	Medium
	Have I enforced as much network segmentation as I possibly can, controlling that only necessary network traffic traverses across control points, and ensuring that systems only have Internet access when absolutely necessary?	Medium
	Do I understand the extortion cyber kill chain, and have I implemented detection and prevention at as many different points in the kill chain as possible, recognizing that each control only has a marginal probability of success?	Medium
	Have I considered my "availability" vulnerabilities and implemented some form of DDoS mitigation for every potentially critical internet system?	Medium
	Do I understand what security controls have failed or are lacking when other businesses fall victim to extortion, and am I confident that my business won't repeat the same obvious mistakes?	Medium
	Does my endpoint solution provide me with a single set of tools to gain visibility and protect all the technologies in my portfolio from one central interface?	Low
	Do I have a strategy for upgrading my MFA from SMS to a system that is time, application or token based?	Low

Detect checklist

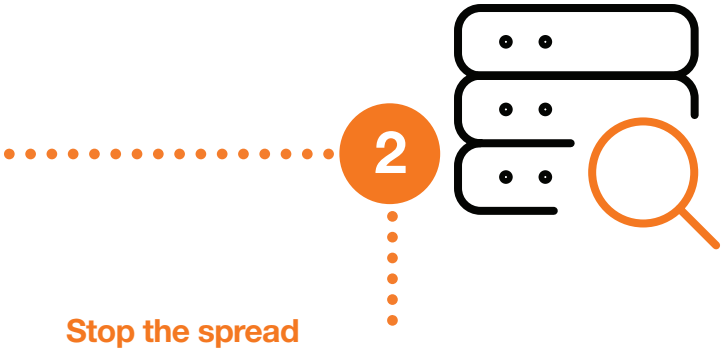
Check	Control	Impact
	Is my endpoint solution cloud-based (if appropriate) and does it allow for continuous monitoring and centralized collection of activity data, along with the ability to perform remote remediation actions, whether the endpoint is on the corporate network or outside of the office?	High
	Am I receiving relevant alerts from all my endpoints, regardless of where they are, and do I have the platforms and processes in place to assess those alerts within a reasonable time and initiate an appropriate response?	High
	Are my platforms and processes configured for a state of “continuous engagement”? Am I responding with enough suspicion and aggression to suspicious or anomalous events, rather than just waiting for the obviously catastrophic ones?	High
	Do I have the skills and resources to properly manage and monitor my endpoint security technology and respond appropriately to suspicious events and incidents when they are flagged?	High
	Do I understand the extortion cyber kill chain and have I implemented detection and prevention at as many different points in the kill chain as possible, recognizing that each control only has a marginal probability of success?	Medium
	Have I investigated the possibility of introducing some form of deception into my detection strategy, so that I am fully exploiting the “homefield” advantage I have over an attacker?	Medium
	Do I have detection sensors and controls in place at multiple diverse places in my infrastructure, e.g. on the network, AD and firewall, so that I’m not just dependent on EDR alerts, which are frequently bypassed?	Medium

Respond

Respond to cyber attacks with proper containment and remediation plans.

Stay calm and keep to the plan

If the worst should happen and you do fall foul of an extortion attack, try and remain calm and don't make rash decisions. Now is the time to initiate your response plan and get control of the situation. **Ideally you should have a retainer in place with a CSIRT that can help coordinate and provide what will be much-needed additional manpower on a 24x7 basis**. A CSIRT should be engaged at the earliest opportunity.



Stop the spread

The first step is t**o identify affected systems and isolate them or their subnets to prevent any further spread**. Disconnect their physical and wireless network connections and remove any connected storage devices, including mobile phones. Do not restart or shutdown the encrypted device as forensic analysis may assist with recovery. Cut internet access initially to prevent any potential command and control communications from the attacker, but **be cautious of disrupting a computer that's in the middle of encrypting data** as this could render the data irrecoverable. Again, your CSIRT should be able to advise you here.

This should give you some time to fully assess the scope of the incident and plan how to recover from it. Identifying the ransomware strain may give you an indication as to who is behind the attack, and their standard TTPs. This may help in discovering what they have targeted.

Keep people informed

Clear, open and honest communication is vital, both internally and externally. Internally, staff need to be made aware of what has happened, what is being done about it and how they can help. If staff understand what is happening, they will be less likely to work around any measures you may put in place to recover and improve security, which could otherwise appear obstructive to their work.

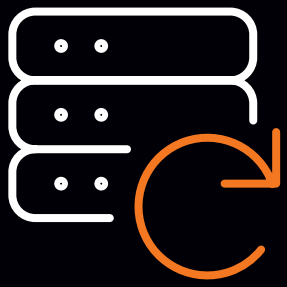
Externally, it is important to take control of the narrative from the outset. Notify the appropriate regulatory bodies and law enforcement agencies as soon as required. In addition, issue a clear, strong public statement explaining what happened, how much you currently know and what you are doing about it. Trying to keep the incident secret will only serve to make you look dishonest and inept when the details do inevitably leak out. The reality of the situation will probably come out in the end as the attackers will release details of the incident, especially if they think they might not get paid.

4

Don't fuel the fire

Do not pay the ransom!! Your stolen data will more than likely end up being released or sold somewhere despite what the attackers say. They are criminals after all. Even if they do provide a working decryptor, they are notorious for struggling with large files, especially databases, so there is no guarantee that all your data can be recovered. Equally, do not engage with ransom negotiators, as they don't necessarily truly have your best interests in mind. While they may well be able to negotiate a lower ransom, their charges often mean that you ultimately pay out more than the initial ransom – and you still have your recovery costs to consider.

5



Establish a trustworthy beachhead

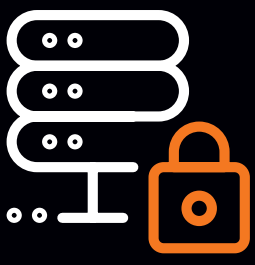
While it's feasible to detect and remove specific malware or hacking tools from a computer, **it's almost impossible to assert that a network is "clean" after it has been infected or compromised**. To fully recover from the attack, and completely evict the attackers from your environment, you should **seriously consider scrapping everything and rebuild the affected networks from scratch**. You should even go as far as recreating your Active Directory domain if domain controllers were compromised.

Although this can clearly be a daunting undertaking, it is the only way to 100% know that the attacker has been removed from your networks as often it is not possible to fully know where an attacker has been and what they have done. Rather than spending the time trying to work that out it will likely be quicker, easier and cheaper to rebuild everything. You also have the opportunity to implement better security controls during the build process. This is where your **secured backups become a critical component** as they should allow you to get mission-critical systems up and running quickly, providing they have not been compromised.

6

Recovery is a marathon, not a sprint

Full recovery from a serious incident can take a long time, and the response effort will claim a huge toll from your team. **Consider the wellbeing of any staff involved in the recovery process**. They will likely be working long hours and care should be taken to ensure they get adequate rest and time off to avoid burn out. This is again where a CSIRT can be crucial as they can provide the additional manpower needed to allow the rotation of key staff needed in the recovery process.



Hope for the best, plan for the worst

Despite your best efforts, **you need to plan for an attacker slipping your defenses and succeeding in encrypting data and disabling systems**. In the worst case, you will only be aware of this after it has already happened, and you may have to respond to the crisis using IT platforms that are crippled or destroyed. Given the possibility of such a nightmare scenario, however remote it may be, here are nine steps to plan for in advance.

1. Secure your backups

Store them offsite and segmented where they will be shielded from destruction in the case of a compromise.

2. Have a response team

Ensure that your response team is well defined, authorized and equipped with what they may need in a disaster.

3. Have a plan

Your response team should be working from a clear playbook that covers as many eventualities as you can anticipate.

4. Plan for reinforcements

It is highly unlikely that you will be able to respond and recover from an extortion incident without the help of expert incident responders and other professionals. It therefore makes sense to have security and IT support vendors selected ahead of time, and perhaps even to have commercial and contractual frameworks in place, in case you need to call on them in a crisis.

5. Keep your contact book updated

You may need to reach out to any number of people internally and externally, including business leaders, incident responders, insurance, law enforcement, suppliers and providers, your legal and communications teams and more. Ensure that you have their latest contact details readily available, even if you can't access your workstation or mobile phone.

6. Have a communications plan

An extortion attack very quickly becomes public, and there is very little you can do to prevent employees, the press and other outsiders from speculating that you may be a victim.

Rather than hide the incident, consider a pre-planned communications strategy designed to reach all your stakeholders, both internal and external.

Think about the level of transparency you are comfortable with and the kind of wording you will use. Assign clear responsibilities and an authorization process that includes stakeholders from IT, security, legal and communications. You also need to think about the channels you will use, as traditional communications platforms like your website, email or social media might not be available to you.

And don't forget your internal stakeholders. Communicating clearly, frequently and transparently with staff is the best way to make them part of the solution during a crisis, rather than part of the problem.

7. Have alternative channels

On the assumption that an extortion attack will cripple your IT in some way, you need to think about how you will go about dealing with the crisis, collaborating and communicating if your core technologies are unavailable or unreliable.

8. Check your morals

Its ethically uncomfortable to negotiate with the criminals. Aside from the negative impact that ransomware payouts have on broader society, your business and your staff will have to make an ethical choice about whether you are willing to pay a ransom, and under what circumstances. It's worthwhile to have this discussion before the actual incident happens.

9. Have a rainy-day fund

A successful extortion incident can cost a lot of money, and not just in the form of the actual ransom. There can be additional costs to be paid for responders, negotiators, brokers, and acquiring cryptocurrency in a hurry. It may be worthwhile to estimate these costs and consider how you would pay them in the event of an incident. How to access large volumes of cryptocurrency is especially something you may want to think about ahead of time.

Just in case:

You can find your country's emergency CSIRT hotline on

orangecyberdefense.com/emergency/

Respond checklist

Check	Control	Impact
	Do I have a clearly documented, reviewed and communicated incident response plan in place that anticipates the worst-case of a successful extortion attack?	High
	Do I have clear plan for turning off or disconnecting computers from the network in the event of a compromise? Does that plan extend to my home workers also?	High
	Do I have a clear communications plan for keeping IT staff, leadership and employees informed about the incident and my response? Do I have a backup plan in case “traditional” channels like email are impacted?	High
	Have I engaged with my legal, communications and marketing teams regarding a strategy for informing customers and the public about an incident?	High
	Do I have a retainer in place with a 24x7 CSIRT who can help me assess the impact, coordinate a response needed additional manpower during the recovery efforts?	High
	Have I gathered intelligence about the experiences of other companies that have fallen victim to extortion attacks, and have I incorporated those lessons into my plan?	Medium
	Has my team had the opportunity to “practice” the plan as a tabletop exercise or under real-life exercise?	Medium
	Do I have an agreement with my legal team, financial team, risk and leadership about the eventuality of having to pay a ransom, and the basis on which a decision to pay might be made?	Low
	Have I engaged with my financial team, legal, risk and leadership about the possible short-term costs of a breach, and what funds and cryptocurrency might be obtained in the worst-case scenario?	Low
	Do I have a strategy for how I will source, manage and remunerate the human resources that may be required for an intensive, multiweek recovery effort?	Low

Conclusion

Cyber extortion attacks are a scourge. The volume and damages are growing at an almost exponential rate. The impact of an incident can be massive, not just for the "direct" victim, but also for the secondary and tertiary victims who may have their private information exposed or depend on the primary victim for products or services. The adversary is highly skilled and motivated, and every business is considered prey for the hunt. Every CISO and security professional should have countering ransomware near the top of their list of priorities.

We've argued in this paper and elsewhere that cyber extortion is a systemic problem emerging from the convergence of an unregulated technology evolution and an established and advanced criminal ecosystem. Ultimately, the problem of cyber extortion can only truly be countered by understanding and affecting these systemic drivers.

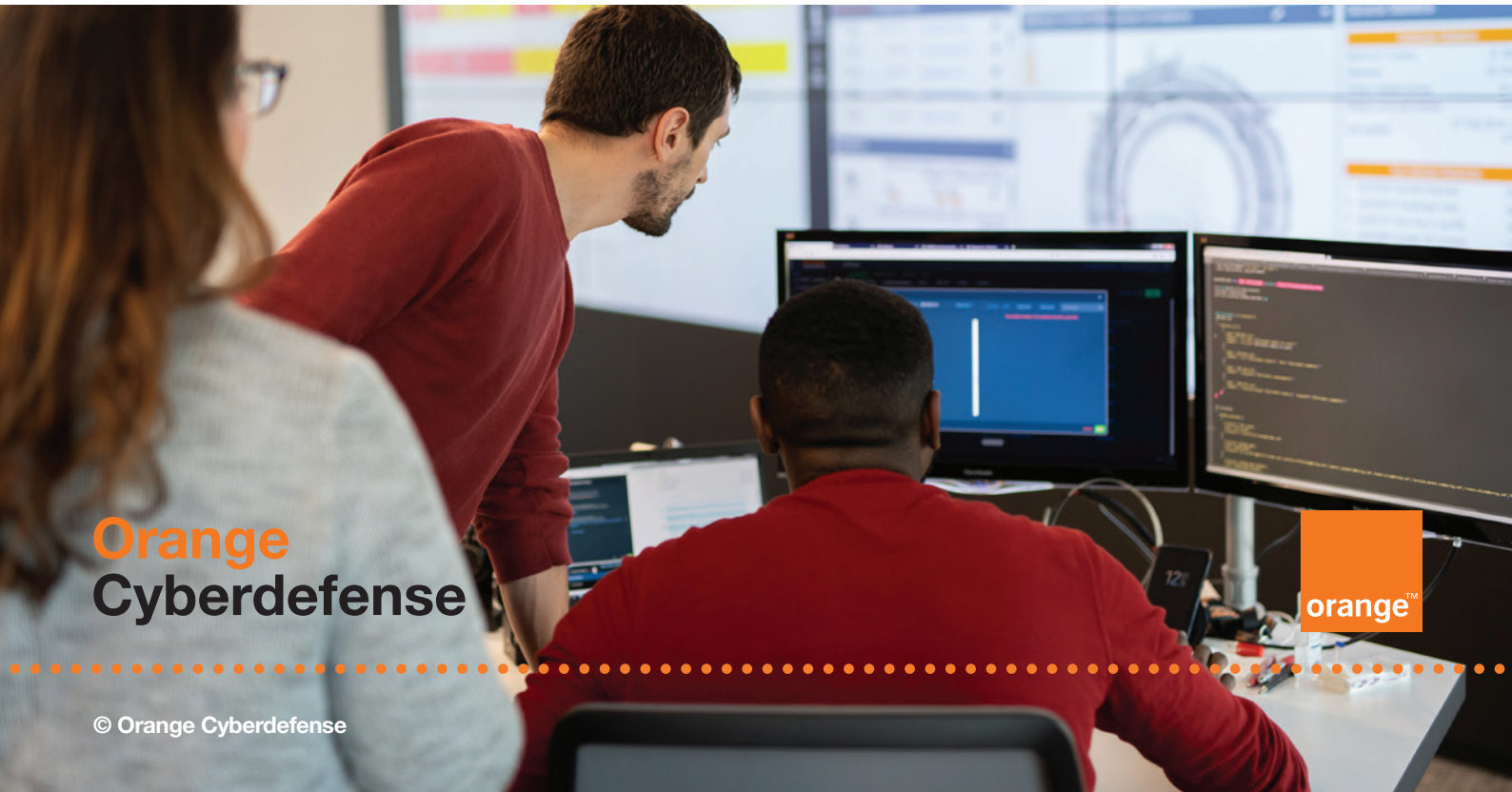
In the meantime, we face an apparently unstoppable threat with no reservations, no limitations and an insatiable appetite for new victims. With the potential consequences mounting and exacerbated by regulatory controls and penalties, we can't afford to wait until the systemic issues are resolved.

Although we can't depend on technology solutions alone to resolve the issue of extortion attacks, we can use technology to impose extra costs on the attacker, slow their rate of movement, minimize the impact of a breach and ensure a rapid and robust recovery.

Extortion attacks are a multi-faceted problem and therefore require a multi-faceted response. None of the controls we discuss in this paper are new or radical in any way, but each additional control adds to the depth of our defense and serves to reduce the probability or the impact of an attack.

In this paper we outline a detailed program of technical and procedural controls that should all be within your reach, organized around our modified version of the NIST cybersecurity framework. The checklists provided serve as a summary of the diverse controls we recommend for each domain of the framework, and can help you prioritize your efforts where they are likely to have the most impact.

None of the controls will individually prevent an extortion disaster, but collectively they will significantly improve your posture and strengthen your cyber resilience. Not only will this greatly improve your position against the ransomware threat, but also improve your general cybersecurity posture overall.



Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection and response services to organizations around the globe.

As Europe's go-to security provider, we strive to build a safer digital society. We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Orange Cyberdefense retains a 25+ year track record in information security. Distributed across the world we have:

- **250+ researchers and analysts**
- **18 SOCs**
- **11 CyberSOCs**
- **4 CERTs**
- **Sales and services support in 160 countries**

We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Orange Cyberdefense has built close partnerships with numerous industry-leading technology vendors. We wrap elite cybersecurity talent, unique technologies and robust processes into an easy-to-consume, end-to-end managed services portfolio.

At Orange Cyberdefense we embed security into Orange Business Services solutions for multinationals worldwide. We believe strongly that technology alone is not a solution. It is the expertise and experience of our people that enable our deep understanding of the landscape in which we operate. Their competence, passion and motivation to progress and develop in an industry that is evolving so rapidly.

We are proud of our in-house research team and proprietary threat intelligence thanks to which we enable our customers to focus on what matters most, and actively contribute to the cybersecurity community, Our experts regularly publish white papers, articles and tools on cybersecurity which are widely recognized and used throughout the industry and featured at global conferences including, Infosec, Manchester DTX, RSA, 44Con, BlackHat and DefCon.

If you have been recently become a victim of ransomware, or not yet, but you wish to discuss your next steps to avoid becoming one, feel free to contact us at **info@orangecyberdefense.com** or visit our Managed Detection and Response page: **https://orangecyberdefense.com/global/all-services/detect-respond/**

We hope you found this whitepaper insightful. Stay safe!

Visit us at: www.orangecyberdefense.com

Twitter: @OrangeCyberDef

Sources:

1. https://www.wordnik.com/words/ransom
2. https://www.wordnik.com/words/extortion
3. https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework
4. https://www.sans.org/blog/insights-6th-annual-sans-security-awareness-report-managing-human/
5. https://www.theregister.com/2021/02/18/cve_exploitation_2_6pc_kenna_security/
6. Ponemon 2018 Endpoint Security Statistics Trends
7. https://twitter.com/singe/status/1382368147869679620?s=20
8. https://metabase.dip.secdata.net/question/575
9. 2021 Security Navigator
10. https://twitter.com/singe/status/1382368147869679620?s=20

Orange Cyberdefense

orange™