Deloitte. 德勤

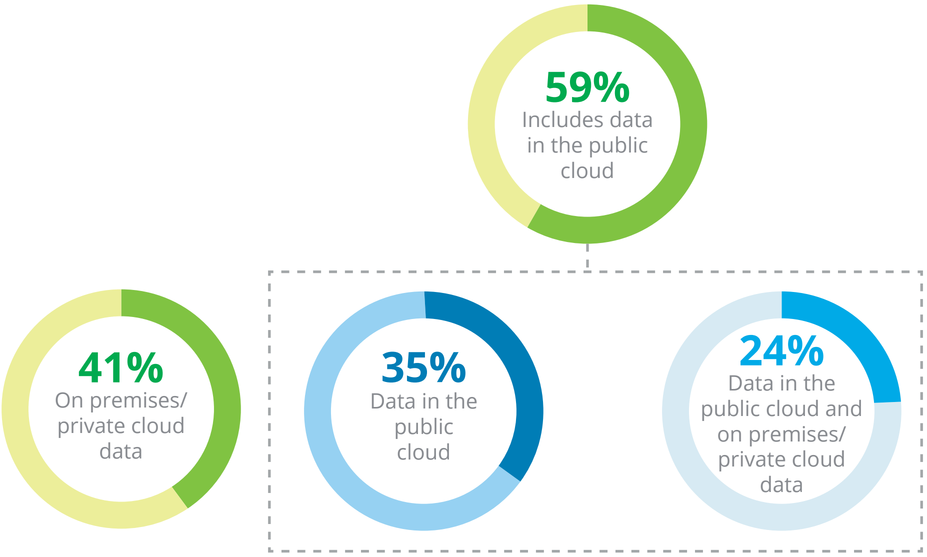
An Anti-Ransomware Strategy

Leading practices to mitigate organizational impact, downtime, and reputational risk

175 MAKING AN IMPACT THAT MATTERS since 1845

As Ransomware[1] continues to evolve, the threat actors' playbook has become more sophisticated, with Ransomware code being bundled and delivered with other malware as part of targeted campaigns to surveil, evade, steal credentials, and exfiltrate data before encrypting files to enhance leverage against victim organizations and provide greater financial gains, commonly referred to as "**DOUBLE EXTORTION**"[2]. Organizations are being targeted by human operated Ransomware attacks[3] for "**BIG GAME HUNTING**"[4] returns and to take advantage of vulnerabilities in systems, applications, and cloud configurations at strategic targets, as nearly six in 10 successful attacks (59%) include data in the public cloud[5]. Commodity malware[6], which has recently been tailored and deployed in COVID-19 themed phishing campaigns, is just one of many ways that enable threat actors to land and expand in organizations' networks, resulting in lateral movement, escalation of privileges, exploitation of vulnerabilities, and data exfiltration.

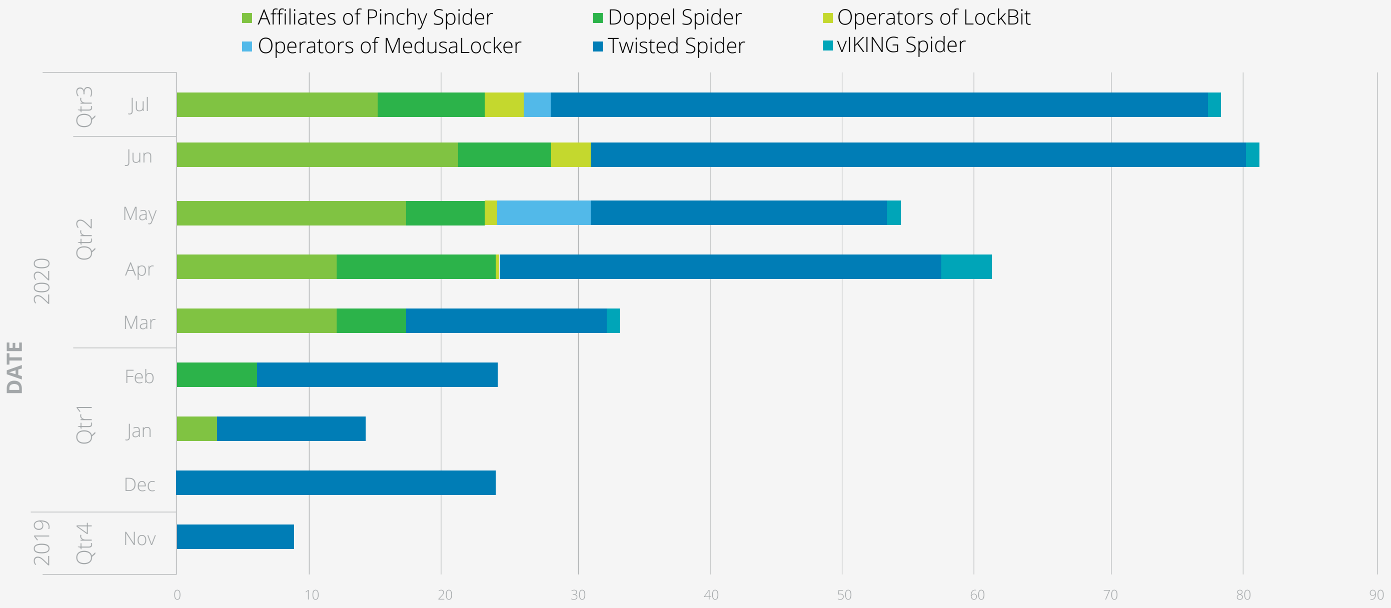
Data in the public cloud is a mainstream target[7]



Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? Responses from respondents whose organization's data had been encrypted in the most recent ransomware attack. Base 1,849 respondents.

Victims Data Leaked by Ransomware Threat Actors[8]

Count of Entities Published to Dedicated Leak Sites by Criminal Adversary



Deloitte's team of Cyber Forensic and Incident Response professionals have analyzed the trends, tactics, techniques, and procedures of threat actors, and correlated threat intelligence from our Cyber team[9] and experience from our Cyber Managed Services professionals, to provide timely, actionable insights, and leading practices that help organizations prepare for and defend against Ransomware attacks.

We are seeing clients adopt and implement the leading practices below based on their operating model maturity and industry threat profiles.

01 **Threat Monitoring**

24/7 monitoring and analytics of security events including triage, incident management, remediation guidance, and tailored Security Information and Event Management (SIEM) content development for industry-specific use cases. Security Orchestration, Automation, and Response (SOAR) for clients with mature playbooks.

02 **Threat Hunting and Response**

Proactive hunting for sophisticated threats that may evade the first line of defence. Hunt activities includes using big data analytics, with Managed Detection and Response (MDR) and Endpoint Detection and Response (EDR).

03 **Threat Intelligence**

Data collection from a variety of internal and external sources to identify client and industryrelevant threats targeting brands, infrastructure, or people.

04 **Incident Response**

Breach investigation, digital forensics, crisis management, privacy advice with incident containment and recovery.

05 **Identity Management**

Managed identity lifecycle for internal and customer identity, access management, identity governance, and privileged access management.

06 **Attack Surface Management**

Vulnerability management, application security management and integration of security controls into the development pipeline with DevSecOps.

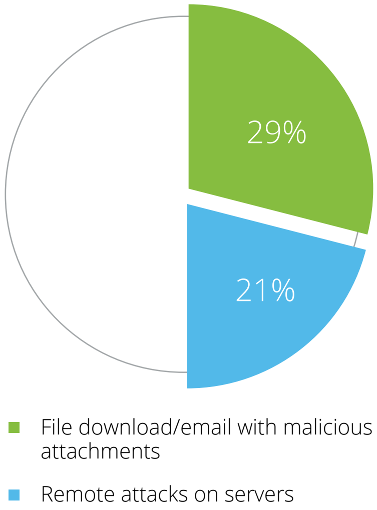
07 **Cloud, Data and Infrastructure Protection**

Cloud platform, host and container protection, cloud platform security compliance monitoring. Data protection with managed encryption, Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB). Infrastructure security covering a range of network, endpoint, web and email security controls.

The Most Common Ransomware Attack Methods

An organization's posture if it suffers a Ransomware attack, and its allocation of resources to resolve vulnerabilities in line with risk tolerances and cyber security program goals and objectives, is critical to successfully preventing and responding to Ransomware attacks. Not all organizations will experience a Ransomware attack, but they must plan for the eventuality and be prepared to respond if an attack occurs. Leading practices we have observed include decreasing the attack surface[10], hardening the perimeter, segmenting or micro-segmenting networks, having least privilege or Zero Trust[11] access policies and controls, effective and timely patch management of IT system vulnerabilities, and network analytics and digital behavior monitoring.

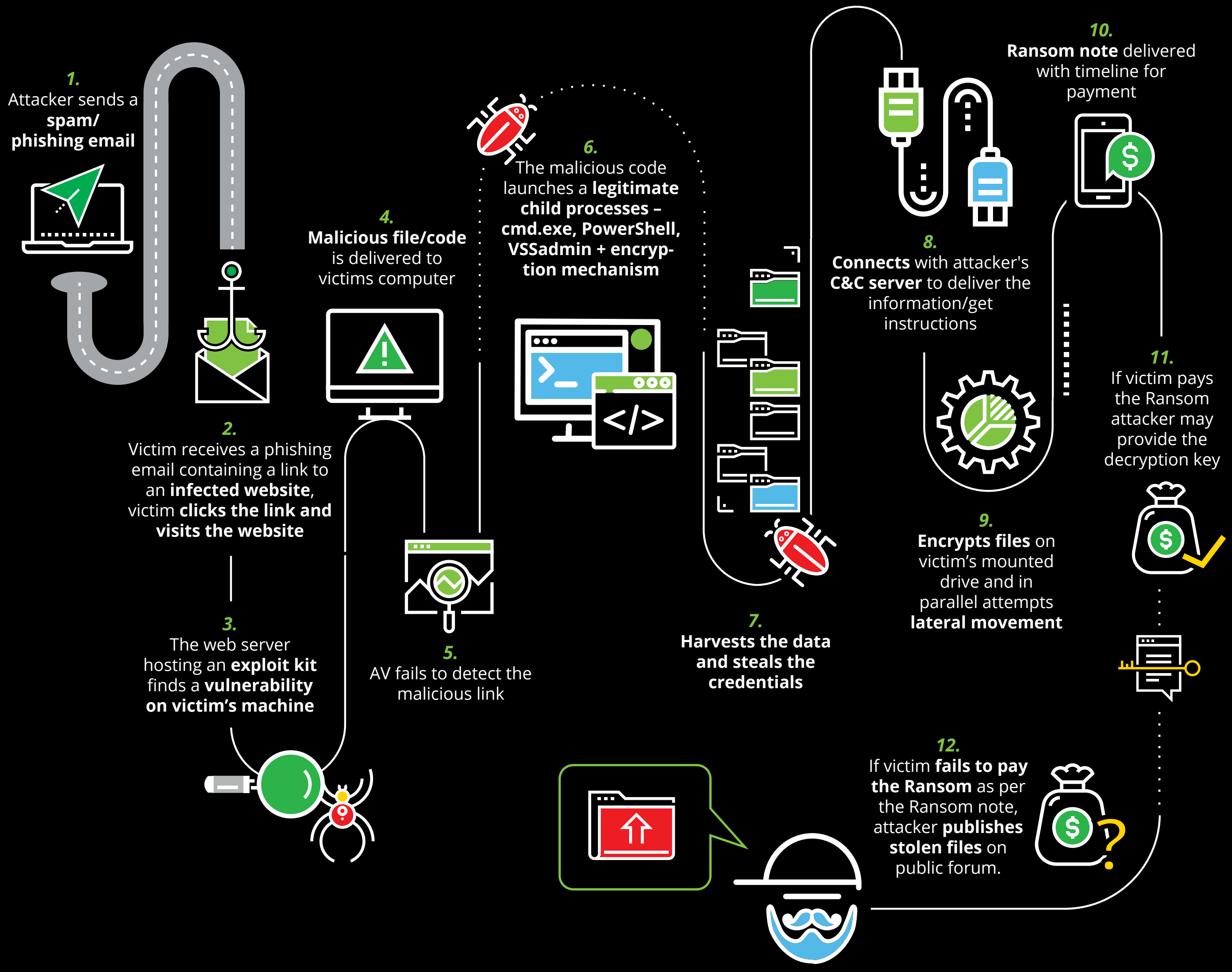
File download/ email with malicious attachments account for 29% and remote attacks on servers account for 21% of Ransomware attack techniques[12]



Phishing Campaigns

Phishing remains the most common and damaging attack method. It increased in use and exploitation as the COVID-19 pandemic took hold across the globe, and many organizations had to quickly transform their operating models to support new work-from-home requirements. As organizations rushed to scale-up existing technologies and bolt-on new solutions to continue to operate, cyber security professionals worked tirelessly – in distributed teams using virtual technologies – to update and modify controls, policies, and procedures. For most organizations, the backlog of work required far exceeded their compliment of available professionals, most of whom had to simultaneously learn how to use new technologies as they were being implemented.

The danger has been exacerbated by threat actors changing tactics to prey on the fears and insecurities of people working from home by sending official looking alerts and email updates that include phishing links and malicious attachments as if they originated from the World Health Organization, the United Nations, and government health agencies. Many organizations are continuing to focus on the people aspect of their operations in terms of restructuring, right-sizing, furloughs, and lay-offs, in order to continue to stay operational, but have yet to fully consider if they have been compromised by targeted phishing campaigns that include dormant Ransomware.



1. Attacker sends a **spam/ phishing email**

2. Victim receives a phishing email containing a link to an **infected website**, victim **clicks the link and visits the website**

3. The web server hosting an **exploit kit** finds a **vulnerability on victim's machine**

4. **Malicious file/code** is delivered to victims computer

5. AV fails to detect the malicious link

6. The malicious code launches a **legitimate child processes – cmd.exe, PowerShell, VSSadmin + encryp-tion mechanism**

7. **Harvests the data and steals the credentials**

8. **Connects** with attacker's **C&C server** to deliver the information/get instructions

9. **Encrypts files** on victim's mounted drive and in parallel attempts **lateral movement**

10. **Ransom note** delivered with timeline for payment

11. If victim pays the Ransom attacker may provide the decryption key

12. If victim **fails to pay the Ransom** as per the Ransom note, attacker **publishes stolen files** on public forum.

As organizations refocus their efforts to prevent successful phishing campaigns, including those related to targeted Ransomware attacks, they should consider:

01 Implementing an email gateway and configuring it to scan and block malicious email, including embedded links and attachments.

02 Implementing URL filtering and blocking and reputational analysis or scoring as this can defang or stop many phishing and other malicious link attacks from delivering their intended payload or exploit code.

03 Reducing the chance of spoofed emails by implementing a Sender Policy Framework ("SPF") or Domain-based Message Authentication, Reporting & Conformance ("DMARC")[13].

04 Configuring firewalls to block known malicious IP addresses.

05 Training employees at least annually on computer, email and internet use, data handling and disposal, and cyber incident reporting and handling.

06 Routine random testing of employees to determine if they are susceptible to phishing campaigns, and where necessary, providing additional resources and training to employees who struggle.

07 Tagging external emails with a warning that they originate outside the organization to give employees additional awareness.

Insecure Network Services

The exploitation of insecure network services, especially Remote Desktop Protocol ("RDP"), is another common attack method used to access an organization's environment. RDP was initially designed as a convenient way to remotely manage Windows servers on the same private network. However, it was not originally intended for use over the internet. Because it is sometimes overlooked or not secured, threat actors often look for, and seek to exploit, RDP where there is external exposure to the internet. To reduce the risk of this exposure, organizations should consider:

01 Comprehensively assessing all externally exposed IT systems and closing down unnecessary ports and services.

02 Consider implementing a Threat Intelligence Gateway ("TIG"). A TIG is a device on the exterior of a network that is updated, sometimes hourly, with an intelligence feed that lists all known malicious IP addresses and domains from which attacks could originate. It then blocks any traffic coming from, or going to, these sources; reducing potentially malicious attack traffic from reaching the network.

03 Configuring RDP, or any remote management service, so it sits behind a remote access gateway, or VPN, with multi-factor authentication where possible.

04 Limiting access to only those who need it, and monitoring for unusual access or digital behavior patterns.

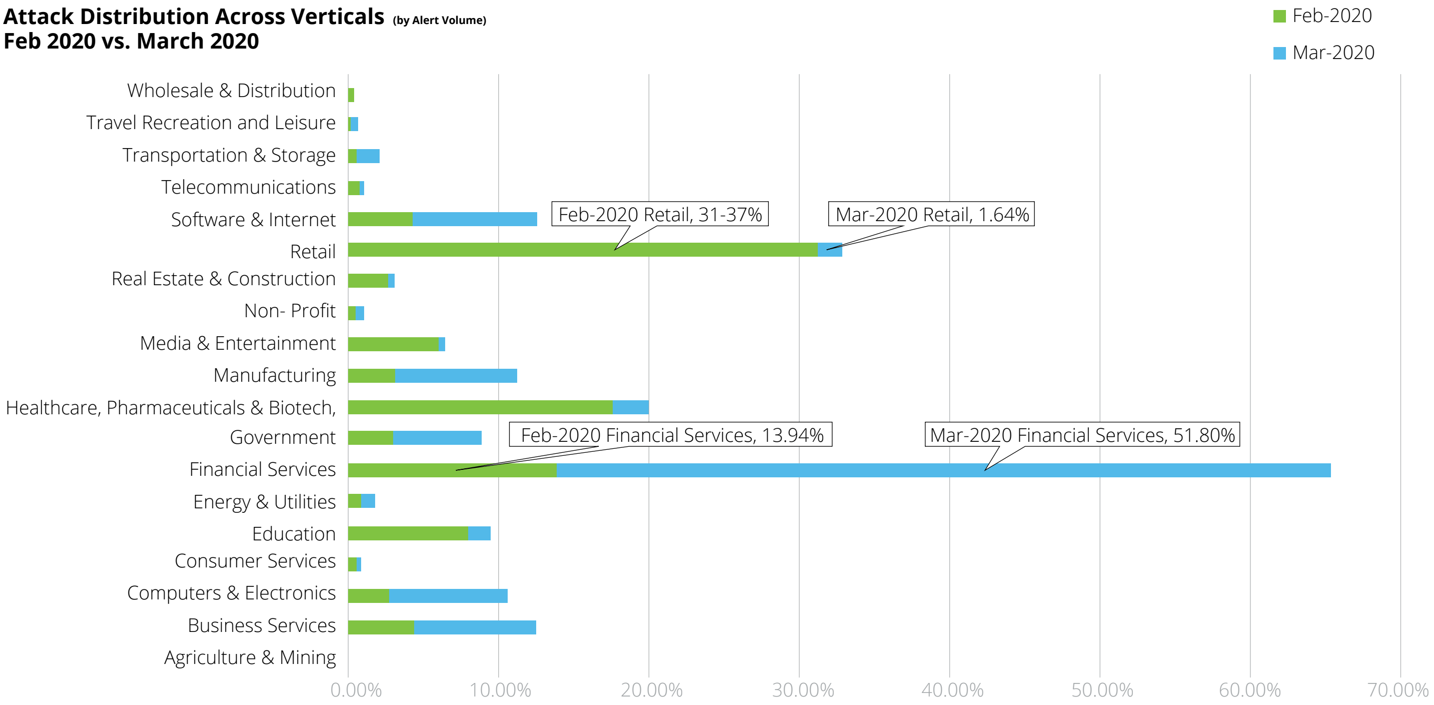
05 Configuring networks to only use Network Level Authentication, which requires users to authenticate before establishing an RDP session.

06 Account lockouts to limit brute-force attacks.

07 Restricting access further through firewall rules that only allow RDP activity from a list of known good or trusted IP addresses.

08 Endpoint detection and response on the RDP server, and monitoring connections and activity using network and digital behavior analysis to flag indicators of compromise and other unusual activity.

Amid COVID-19, Global Organizations Saw a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted[14]



Unpatched Vulnerabilities & Exposures

Common Vulnerabilities and Exposure ("CVE") lists help organizations identify and secure publicly disclosed vulnerabilities[15]. Once a CVE is disclosed, threat actors have a window of opportunity to exploit the vulnerability before hardware and software manufacturers develop and issue patches for it, and these are made available for application to affected hardware and software. Unfortunately, the window of opportunity between when a CVE is disclosed and ultimately patched can be lengthy, and depending on the nature of the unpatched vulnerability, it can have substantial organizational impact and in some cases cause cascading sector, industry, regional, or global damage, as was the case with the WannaCry and NotPetya Ransomware in the summer of 2017.

Unpatched vulnerabilities in Windows Shares (SMB) (CVE-2020-0796)[16], PulseVPN (CVE-2019-11510)[17], F5 Big IP (CVE-2020-5902)[18], Palo Alto Global Protect (CVE-2020-2034)[19], MS RDP (BlueKeep) CVE-2019-0708[20], Palo Alto CVE-2020-2021[21] and Citrix NetScaler (CVE-2019-19781)[22], to name just a few, are still being exploited today.

To reduce the risk of exposure, organizations should consider:

01 Establishing, implementing, and managing a secure configuration for each system on their network.

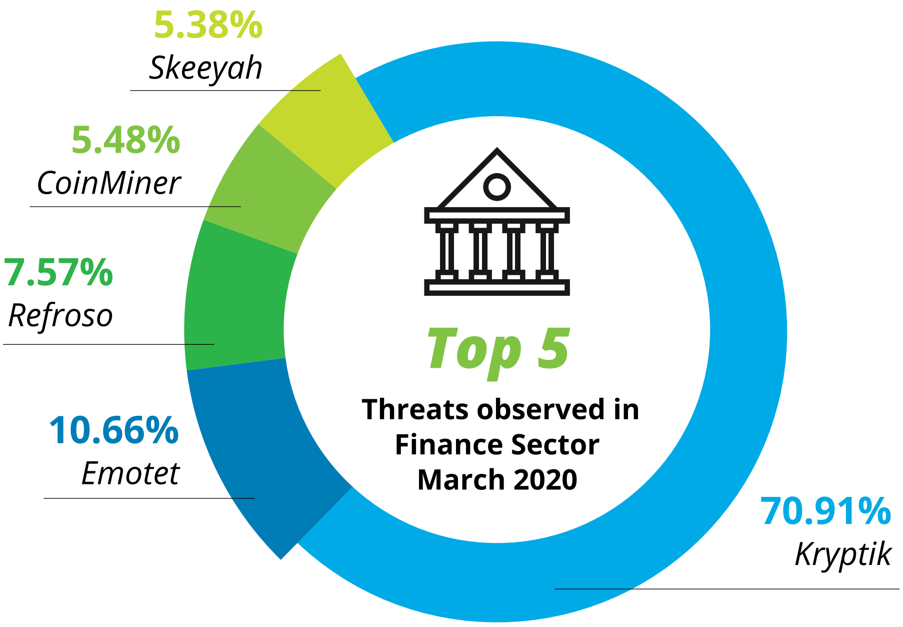
02 Regular review and confirmation that proper access controls are enforced on all externally-exposed IT systems.

03 Processes to maintain current software and firmware versions on all IT systems on a prioritized basis.

04 At least quarterly vulnerability scans of all high-priority and critical IT systems and applications. Prioritizing the remediation of all high severity vulnerabilities between assessments.

05 Least privilege access or Zero Trust policy and controls; particularly with respect to critical information, systems, and digital assets.

06 Scanning for and removal of Windows SMB that is exposed to the internet.



Of the 52% of attacks targeting the financial services sector in March 2020, **70.9% of those came from the Kryptik trojan**, which attempts to target victim machines via nefarious installers. The Kryptik trojan can be very persistent and, without the appropriate visibility, can be difficult to detect as it often deletes its executable file after running.[23]

Least Privilege Access & Monitoring

Whether the initial entry point is a phishing email, exploitation of a vulnerable system, or another attack method, the threat actor's goal is to gain entry and escalate access privileges. Of all the things organizations can do to protect their environments, leading practices to secure and manage least privilege and administrative access are critical to mitigating the risk of a Ransomware attack and exfiltration of information from IT systems.

When threat actors obtain valid system administration credentials, or worse, domain administration credentials, an organization's IT systems and digital assets are at risk of compromise. **Domain administration credentials provide threat actors with the "key to the city"**, and it can be very challenging to regain control after such a severe compromise of IT systems.

Unfortunately, experience shows that many organizations have cyber security postures, controls, and programs that do not rigorously protect administrative and privilege access to their IT systems or digital assets. It is not uncommon to find default and weak passwords being used on endpoints, for example, to facilitate convenience and ease of fulfilling IT service requests by in-house teams. The following leading practices can materially hinder the ability of threat actors to gain administrative and privileged access rights in an organization's IT systems.

01 **Knowing what rights exist and who has them is the first step to protecting administrative and privileged access rights. It can be easy for organizations to overlook administrative privileges on unique systems, network devices, IoT, or other systems. It can only take one system with overlooked administrative credentials set to default, or a weak password, for a threat actor to exploit and gain the level of access they need to carry out their attack.**

Inventorize systems on the organization's network and identify all administrative or privileged accounts.

Identify who has access to each account and determine if they truly need those rights to do their jobs.

Determine the purpose of service accounts, which services they run, which systems they access, and how often.

02 Once administrative and privileged access to an organization's environment is confirmed, implement least privilege access and control.

Restrict the number of people with administrative or privileged access to only those that need it for their jobs. The best way to do this is to implement additional controls in an Identity and Access Management ("IAM") solution that identifies administrative and privileged roles, enforcing the defined policy and facilitating regular auditing for continued access.

Restricted access to **END USER** systems. No employee should log-in to their standard workstation with administrative credentials. Further secure these systems with a strong security policy including restricting access to Registry Editor for Windows end user systems.

Ensure every ID with elevated privileges is unique and follows a robust password policy.

Ensure all service accounts are configured with only the minimum privileges necessary to do their intended job.

Implement multi-factor authentication ("MFA") for all privileged and administrative access IDs. If a threat actor can compromise an administrative ID, MFA makes it challenging for them to take advantage of it.

Prohibit personnel with administrative access from signing on to their normal employee workstations with elevated privileges. Every employee, including IT staff, should be given a standard user access account with restricted or least privilege access on their normal workstation.

Restrict administrative privileges for use necessary to complete a task that requires elevated privileges. This can be accomplished through Privilege Access Management ("PAM") solutions, which require an employee to request escalated privileges and approve access only for the time required to complete the work.

If an organization does not have a PAM solution, consider restricting administrative access and tasks to a jump server or privileged access workstation ("PAW") that is isolated from the internet, securely configured, locked down, and designated as the place for administrative access. Ensure policy defined on the PAW prohibits administrative access log-in on the workstation that is continuous or applies to any system.

03 **After incorporating leading practices in relation to least privilege and administrative access and controls, organizations need to design, tailor and implement monitoring routines and analytics to collect, aggregate, and correlate logs, artefacts, threat intelligence, digital behaviors, and anomalous activity or trends that indicate a potential compromise of IT systems. Several target operating models, subject matter experts, and vendors can be used to optimize Ransomware attack mitigation to provide actionable insights across an organization while limiting data volume and false positives.**

Endpoint Detection & Response

Advanced endpoint detection and response ("EDR") solutions use proactive techniques, such as machine learning and behavioral analysis, to identify potential new or complex threats. EDR solutions properly deployed and configured can quickly identify a Ransomware attack, its scope across endpoints being monitored, and isolate and/or quarantine infected systems to contain the attack. These advanced techniques make it much more difficult for threat actors to establish a solid footing in an organization's network.

If an EDR solution is not deployed on all network endpoints, deployment should be configured and managed to address and mitigate the greatest threats. It should also be configured to protect the organizations most critical IT system and digital assets, and tuned to take full advantage of its capabilities while minimizing false positives.

Organizations can consider isolating endpoints that are not subject to EDR monitoring. For example, SCADA and legacy systems and applications that do not require internet access should be segmented using communication protocols that are carefully reviewed to authorize only necessary data flows within the network. Unnecessary services should be disabled and least privilege or Zero Trust access and controls should be implemented.

Business Continuity & Incident Response Plans

Despite the best laid plans and investments in people, processes, and technology to mitigate organizational risk, there is no 100% guarantee that organizations will not face a Ransomware attack. However, with the proper planning and implementation of leading practices, organizations can minimize downtime and recover more quickly, reducing their operational losses and reputational damage. Leading practices to prepare for an imminent Ransomware attack include:

01 Reviewing Business Continuity and Disaster Recovery plans to critically assess if back-ups of critical systems, applications, data, and digital assets have redundancies online, offline, and offsite. If Ransomware has encrypted an organization's assets, there may be no publicly available decryption key, leaving it with few options to resolve the attack quickly outside of paying the ransom. In many Ransomware attacks, code looks for online and accessible back-ups and disables, deletes, or encrypts these as well.

Leading practice is to implement a secure back-up policy and process involving multiple copies, some of which are offline, offsite, and encrypted. Many organizations leverage traditional tape back-ups with offsite storage in addition to cloud-based back-ups. Regardless of policy or process, all back-ups should be secure and have restricted access protocols.

It is also leading practice to routinely test an organization's ability to recover quickly using back-ups. Mock drills should be planned at least twice a year to recover different critical systems and data across the organization on a rolling basis. Frequently, organizations learn during a Ransomware attack that what they thought was a robust back-up for their critical systems, applications, and data is too slow, resulting in substantial organizational impact, or worse is incapable of recovery, resulting in costly rebuilds and the re-creation of lost critical data.

02

Every organization should have an incident response plan for Ransomware attacks. Leading practice is for these plans to define who is involved in responding to an attack, what responsibilities they have, important support contacts, and a response and recovery protocol. Organizations that have well-thought out, well defined plans, and have practiced execution through table-top and other mock exercises avoid common pitfalls and panic-driven decisions, resulting in quicker overall responses at much less cost. Some key elements considered leading practice in preparing for a Ransomware attack are:

Incident response plans that include all roles, internal and external, which could be involved in a Ransomware attack, based on a well-thought out playbook. This should include key vendors and contacts, outside firms that can assist with forensics and legal needs, and other counter measures to identify, contain, remediate, and recover.

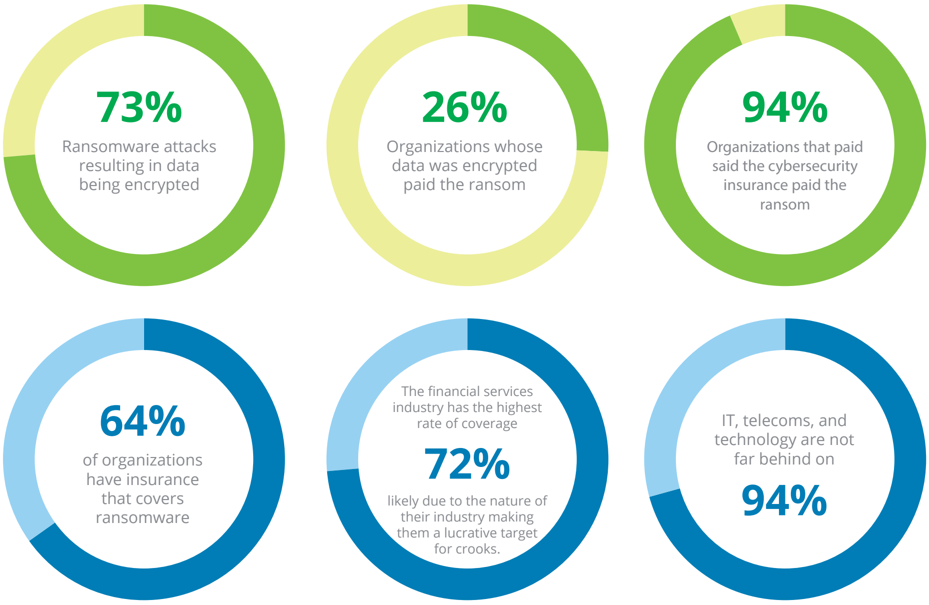
Pre-qualifying and retaining preferred vendors before a Ransomware attack occurs. This enables organizations to tap into those resources on an on-call basis, rather than have to first negotiate and agree contractual terms, conditions, rates, and secure specialized resources DURING an attack. Many external advisors, including Deloitte, prefer to be retained in advance and will make investments at no cost to an organization to best prepare for an attack and minimize the response effort, downtime, and organizational impact.

Practice, practice, practice. Many organizations undertake the design and development of an incident response plan and accompanying playbooks pursuant to edicts from executive management or their boards of directors. However, once complete, these plans and playbooks are shelved and collect dust until an attack occurs. Their effectiveness can degrade rapidly as people, processes, and organizational structures, and attackers' tactics, techniques, and procedures change. Leading practice is to conduct tabletop exercises routinely throughout the year, where organizations can pull together all required personnel, and third party vendors as appropriate, to simulate an actual ransomware event and ensure their tools, processes, methods, and people are prepared. The more an organization practices, the more it will identify ways to improve its plan, train its people, reduce confusion, frustration and panic when an attack occurs.

Conclusion

Ransomware can be costly and damaging to an organization that does not actively protect itself or is ill-prepared for the realities of an attack. As this type of attack increases in frequency and continues to evolve, it is critical that organizations are aware of the latest successful attack patterns and what they can do to reduce exposure. By following leading practices, organizations can lower the probability of a successful Ransomware attack, and mitigate associated risks in terms of response effort, downtime, organizational impact, costs, and reputational damage. Moreover, issuers of leading Cyber Risk insurance policies, include access to pre-loss services that could enhance and enrich organizations' readiness to respond to an attack. Organizations should consult their Cyber Risk policy issuers and brokers to understand the potential benefits including if their policy covers payment towards ransom.

Cybersecurity insurance and ransom payments[24]



End Note

This white paper includes some of our observations and perspectives to help organizations benefit from and put into action leading practices that are appropriate for their environments and cyber security posture. However, it does not address all known risks or applicable mitigation tactics. It should be used as a guide only, and be one of several resources that organizations use to review and tailor their cyber security posture to meet their program goals and objectives.

1. Ransomware is a type of malware that prevents you from accessing your computer (or the data that is stored on it). The computer itself may become locked, or the data on it might be stolen, deleted or encrypted. Some ransomware will also try to spread to other machines on the network, https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
2. https://www.hkcert.org/my_url/en/blog/20071301
3. https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
4. Big-game hunting is the process of cybercriminals focusing on high-value data or assets within businesses
5. https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf
6. Commodity malware – malware that is widely available for purchase, or free download, which is not customised and is used by a wide range of different threat actors.
7. https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf
8. https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
9. Deloitte's global network of Cyber Intelligence Centers operate 24/7 to provide advanced security operations including Threat Intelligence, Threat Monitoring, Threat Hunting and Security Analytics
10. https://whatis.techtarget.com/definition/attack-surface
11. https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/zero-trust-adoption-not-slowed-by-pandemic.html
12. https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf
13. https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (Accessed December 08, 2020)
14. https://www.carbonblack.com/blog/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/
15. Common Vulnerabilities and Exposures (CVE®) List and the associated references are sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2020, The MITRE Corporation. CVE and the CVE logo are registered trademarks of The MITRE Corporation.
16. NIST National Vulnerability Database, National Institute of Standards and Technology, https://nvd.nist.gov/vuln/detail/CVE-2020-0796 (Accessed December 08, 2020)
17. NIST National Vulnerability Database, National Institute of Standards and Technology, https://nvd.nist.gov/vuln/detail/CVE-2019-11510 (Accessed December 08, 2020)
18. NIST National Vulnerability Database, National Institute of Standards and Technology, https://nvd.nist.gov/vuln/detail/CVE-2020-5902 (Accessed December 08, 2020)
19. NIST National Vulnerability Database, National Institute of Standards and Technology, https://nvd.nist.gov/vuln/detail/CVE-2020-2034 (Accessed December 08, 2020)
20. NIST National Vulnerability Database, National Institute of Standards and Technology, https://nvd.nist.gov/vuln/detail/CVE-2019-0708 (Accessed December 08, 2020)
21. NIST National Vulnerability Database, National Institute of Standards and Technology, https://nvd.nist.gov/vuln/detail/CVE-2020-2021 (Accessed December 08, 2020)
22. NIST National Vulnerability Database, National Institute of Standards and Technology, https://nvd.nist.gov/vuln/detail/CVE-2019-19781 (Accessed December 08, 2020)
23. https://www.carbonblack.com/blog/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/
24. https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

Contacts

Richard Kershaw
Partner
+852 2740 8808
rwkershaw@deloitte.com.hk

Miro Pihkanen
Partner
+852 6022 5231
miropihkanen@deloitte.com.hk

Brian Wilson
Partner
+852 6800 0590
brianwilson@deloitte.com.hk

Puneet Kukreja
Partner
+852 54030969
puneetkukreja@deloitte.com.hk

Jimmy Mate
Director
+852 6283 6958
jmate@deloitte.com.hk

Chad Olsen
Partner
+852 2238 7647
chaolsen@deloitte.com.hk

MAKING AN
IMPACT THAT
MATTERS
since 1845

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the “Deloitte organization”) serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 330,000 people make an impact that matters at www.deloitte.com.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

The Deloitte brand entered the China market in 1917 with the opening of an office in Shanghai. Today, Deloitte China delivers a comprehensive range of audit & assurance, consulting, financial advisory, risk advisory and tax services to local, multinational and growth enterprise clients in China. Deloitte China has also made—and continues to make—substantial contributions to the development of China's accounting standards, taxation system and professional expertise. Deloitte China is a locally incorporated professional services organization, owned by its partners in China. To learn more about how Deloitte makes an Impact that Matters in China, please connect with our social media platforms at www2.deloitte.com/cn/en/social-media.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

BJ-04EN-20

This is printed on environmentally friendly paper