CrowdStrike eBook

CROWDSTRIKE

SECURING TODAY'S DISTRIBUTED WORKFORCE

Resources for Ensuring Optimal Security During the Global Pandemic

TABLE OF CONTENTS

Foreword

Message From CrowdStrike CEO George Kurtz

Let me start by expressing on behalf of the global CrowdStrike® team how grateful we are to the healthcare workers, law enforcement and first responders — and all individuals whose jobs require them to put themselves at risk to keep the rest of us as safe and healthy as possible. In addition, our hearts go out to everyone whose family and loved ones have been affected by this devastating outbreak.

As CrowdStrike's CEO, my first responsibility is to our people and the communities where we live and work. To that end, I have directed all CrowdStrike employees to do their part by working at home and eliminating unnecessary travel, and to abide by all local and federal health guidelines to help slow the spread of this highly infectious disease.

Our next responsibility is of course to our customers, and on this front we have many successes to share. One thing I would like to make clear: We believe that CrowdStrike has an extremely important role to play in this crisis.

The widespread health and economic impact of the new coronavirus has not deterred cyber adversaries. In fact, quite the opposite is occurring. In times of crisis, adversaries often try to exploit the situation, prey on the public's fear and escalate attacks. I know it is difficult to imagine, but we are seeing nation-state adversaries and e-criminals launch phishing campaigns using the coronavirus as bait. We expect this to escalate, and we are tracking the spread of these malicious campaigns.

Our disruptive cloud-native approach is uniquely suited to helping customers stay ahead of these emerging threats, whether their workers are at home, in the office or operating entirely in the cloud.

To extend our ability to aid the CrowdStrike community, we launched a **coronavirus surge relief plan** that allows our customers to surge the number of endpoints protected by the CrowdStrike Falcon® platform for up to 60 days. This enables existing customers to quickly onboard new remote workers without having to worry about a procurement cycle. Additionally, we launched the **CrowdStrike Falcon Prevent™ for Home Use program**, which allows company administrators to immediately install our next-generation endpoint protection on employees' home and personal systems for a limited time. These free-of-charge programs have been extremely well received by our customers in their time of need.

For organizations of every size, industry and location, empowering employees to immediately start working from home is no trivial matter. Particularly for big organizations, managing this change quickly and efficiently can present major challenges. CrowdStrike is fortunate in this respect, since we are a company built from inception to thrive with a remote workforce. On a regular basis, approximately 70% of our employees already work remotely. As a result, we do not expect any disruption in our operations or ability to support our customers as we transition the rest of our workforce to a work-from-home model.

For many of our customers, it's not so simple, and it's important to note that as organizations move their workforce outside of physical offices, their attack surface grows exponentially. They may need to rapidly provision fleets of new endpoints, such as laptops and mobile devices, and spin up new cloud workloads, while ensuring that every workload everywhere is protected with real-time security, even when the user is offline.

To put this in perspective, one of our large enterprise customers recently rushed to buy 12,000 laptops to deploy to newly remote employees. CrowdStrike can play a key role in these types of deployments, because the security challenges associated with a remote workforce are best solved by a cloud-native security platform. A true cloud-native platform like CrowdStrike Falcon does not require physical infrastructure. It allows customers to easily and remotely install, manage and protect their workloads at scale, no matter where their employees are located.

During times like this, the best companies continue to innovate and focus on customer success. This allows them and their customers to emerge from a crisis even stronger than before. Cybersecurity has been and will remain mission-critical to organizations, to provide business resiliency, and just as importantly, peace of mind to reassure their employees and customers that they are protected, so they can continue to focus on the things that matter most.

If there is anything that CrowdStrike can do to help your organization stay safe and secure in this time of need, please don't hesitate to reach out to us. We have a saying here at CrowdStrike: "One team. One fight." We are truly in this together.

Chapter 1
Keys to Embracing and Securing a Remote Workforce

by CTO **Mike Sentonas**

The declaration of a global pandemic by the **World Health Organization (WHO)** underscores what we are all coming to realize: that the COVID-19 disease, caused by a new variation of the coronavirus, has caused a level of social and economic upheaval that is unprecedented in modern times. Organizations are facing sudden and profound challenges as they seek ways to quickly support corporate directives for employees to vacate offices and corporate campuses and start working from home. Maintaining security in the face of this global office exodus presents significant risks for most organizations.

Challenges of Quickly Adopting a Remote Workforce Model

Globally, 50% of employees are working outside of their main headquarters for at least 2.5 days per week, according to the latest International Workplace Group report. However, COVID-19 is challenging more — perhaps all — organizations to potentially embrace a remote work style immediately. Aside from the pressure this office exodus puts on IT teams, network architectures and even equipment suppliers, there are real cybersecurity challenges organizations need to consider.

Six key factors that can help ensure remote worker cybersecurity:

- **Make sure you have a current cybersecurity policy that includes remote working.** Strong security policies may already exist, but it is important to review them and ensure they are adequate as your organization transitions to having more people working from home than in an office. Security policies need to include remote working access management, the use of personal devices, and updated data privacy considerations for employee access to documents and other information. It is also important to factor in an increase in the use of shadow IT and cloud technology.

- **Plan for BYOD (bring your own device) devices connecting to your organization.** Employees working from home may use personal devices to carry out business functions, especially if they cannot get access to a business-supplied device as supply chains may slow down. Personal devices will need to have the same level of security as a company-owned device, and you will also need to consider the privacy implications of employee-owned devices connecting to a business network.

- **Sensitive data may be accessed through unsafe Wi-Fi networks.** Employees working from home may access sensitive business data through home Wi-Fi networks that will not have the same security controls — such as firewalls — used in traditional offices. More connectivity will be happening from remote locations, which will require greater focus on data privacy, and hunting for intrusions from a greater number of entry points.

- **Cybersecurity hygiene and visibility will be critical.** It is not unusual for personal devices to have poor cybersecurity hygiene. Employees working from home can result in an organization losing visibility over devices and how they have been configured, patched and even secured.

- **Continued education is crucial, as coronavirus-themed scams escalate.** **WHO** and the **U.S. Federal Trade Commission (FTC)** have already warned about **ongoing coronavirus-themed phishing attacks** and scam campaigns. Continuous end-user education and communication are extremely important and should include ensuring that remote workers can contact IT quickly for advice. Organizations should also consider employing more stringent email security measures.

- **Crisis management and incident response plans need to be executable by a remote workforce.** A cyber incident that occurs when an organization is already operating outside of normal conditions has a greater potential to spiral out of control. Effective remote collaboration tools — including out-of-band conference bridges, messaging platforms and productivity applications — can allow a dispersed team to create a "virtual war room" from which to manage response efforts. If your organization's plans rely on physical access or flying in technicians for specific tasks (e.g., reimaging or replacing compromised machines), it may be prudent to explore alternate methods or local resources.

Ensuring Security Across Your Remote Workforce

CrowdStrike is uniquely well-positioned to provide assistance to companies grappling with this sudden shift to a remote workforce for two reasons: First, our cloud-delivered platform and lightweight agent architecture is ideally suited to supporting and specifically securing remote workers; second, we as a company support a broad and widely dispersed remote workforce ourselves, so we have deep institutional knowledge of how to do so securely and effectively.

Cloud-Native Security

Below are several capabilities the cloud-native CrowdStrike Falcon platform can give you to help make a rapid transition and ensure security as you move your workforce from office to home:

Harness the cloud's scalability and cost-effectiveness. Architecture that is built for the cloud from the ground up flexes with the demands of customers and provides enormous storage and computing power to drive real-time protection, regardless of where your employees are connecting from. Working with a cloud security architecture ensures that additional resources can be provisioned as needed. And as you pivot to support remote employees, there is no need to plan, prepare and provision hardware and software to keep pace.

Gain the highest level of security regardless of where your employees are located. Having a 100% cloud-delivered security architecture ensures that you can protect every workload everywhere, including workloads outside of the firewall, even if they are offline, and provide real-time security functionality with the highest level of efficacy along with compliance status information. **Threat hunting** across every device, especially those that are not on the network, is critical. Achieving this easily — with data accessible instantly and from anywhere — can only be accomplished with a native cloud-delivered solution.

Rely on simple security architecture that delivers comprehensive visibility. Knowing who and what are on your network is foundational to proactive security management. It is critical to have complete visibility of every device connecting to the network regardless of where it is connecting from. With CrowdStrike Falcon's single lightweight agent, there is no requirement to reboot to install; there is minimal impact on runtime performance; there are no "scan storms" or invasive signature updates to impact end-user experience; and users can be secured within seconds.The Falcon platform's continuous and comprehensive workload monitoring and discovery give security teams full visibility of every device: This includes on-premises devices, remote office and home devices, and cloud workloads. This visibility also extends protection across containers and mobile devices.

Ensure worry-free security with endpoint protection delivered as a service. With CrowdStrike Falcon Complete™, customers can entrust the implementation, management and **incident response** of their **endpoint security** to CrowdStrike's proven team of security experts. The result is an instantly optimized security posture without the burden, overhead and cost of managing a comprehensive endpoint security program, thereby freeing up internal resources to work on other projects. **Falcon Complete** is a 100% hands-off and worry-free endpoint protection solution that uniquely provides the people, process and technology required to handle all aspects of endpoint security, from onboarding and configuration to maintenance, monitoring, incident handling, and remediation, regardless of whether it is an on-premises workload or a remote worker.

The COVID-19 crisis and its impact is likely to be with us for a while. Organizations and their employees will be forced to make tough decisions rapidly, and enabling a remote workforce is one of those decisions. There are risks involved in quickly enabling and managing a remote workforce, but the security of your networks, devices and data shouldn't be among them.

Chapter 2
Cyber Threats Heightened by COVID-19 and How to Protect Against Them

by VP of Intelligence **Adam Meyers**

As the COVID-19 pandemic continues to take hold in various geographical locations, government and businesses are rapidly changing how and where they operate to ensure the safety and health of their employees, customers and partners. This environment is dynamic, and the continually shifting paradigm has significant consequences on organizational security posture. "Work from home" is becoming the new normal for organizations hoping to flatten the curve of the pandemic. For some organizations, remote work has been ongoing for several years, and the new push is simply a matter of scaling up existing solutions and policies. In many other environments, work from home is a foreign concept; technology, operations and policies are not prepared for this new reality, and several challenges are being encountered such as:

- Use of personal devices and email for business or handling sensitive information
- Provisioning corporate assets to support remote working arrangements
- Proper deployment and configuration of remote services, corporate VPNs (virtual private networks) and related two-factor authentication methods

Adversaries are keenly aware of these challenges and the opportunities for abusing this situation to their advantage. This chapter provides an overview of tactics and observed cyber threats beginning in January 2020 through publication. The appendix at the end of this eBook lists recent adversary activity observed and will be periodically updated.

Tactic Highlight: Phishing

Phishing remains the primary initial access vector for a variety of **threat actors**. Successful phishing attacks frequently play to greed or fear in the victim. The infamous "Nigerian Prince" schemes are an example of the use of greed, where the promise of riches entices the victim to do things they ordinarily wouldn't do. In the case of the COVID-19 pandemic, fear abounds, and the awareness of the pandemic itself is global. Phishing attacks promise new information about the virus or updates on official guidance.

In addition to what has been observed, CrowdStrike Intelligence assesses with high confidence that it is likely for additional **phishing campaigns to make use of lures aligned with health guidance, containment and infection-rate news** to increase over the next few months.

In addition to phishing lures leveraging health-related interest, there is also a possibility that actors could take advantage of more employees working from home, and move toward lures attempting to spoof company guidance and procedures, human resource correspondence and company IT issues and resources.

Targeted intrusion adversaries in particular have relied on job-themed and human resource-themed lure documents over the last few months. In a situation where employees will increasingly rely on email communications to continue business operations, the threat of phishing campaigns attempting to mimic official business communications will likely increase.

Observed Activity: eCrime

As the pandemic continues to evolve, CrowdStrike has observed sustained eCrime activity across the board, including some with COVID-19 themes. Campaigns have been observed in multiple languages, using multiple attachment types and various levels of COVID-19 information, demonstrating that the scope of these campaigns has been and is likely to remain wide. COVID-19-themed activity has followed the path of the virus as it has moved from Asia across the world. As news about the situation in various locales emerges, the themes and targets change — for example, with news of the COVID-19 situation in Italy, WIZARD SPIDER was observed deploying dynamic web inject files that solely target customers of Italian financial institutions, with the intent of stealing credentials for accounts.

One of the earliest eCrime actors to capitalize on the COVID-19 outbreak was **MUMMY SPIDER** in late January 2020. This actor used Japanese-language spam spoofing a public health center in order to distribute the Emotet downloader malware, which subsequently led to the download and install of **WIZARD SPIDER's TrickBot**.

CrowdStrike Intelligence has continued to identify multiple campaigns distributing additional eCrime threats, such as Gozi ISFB, Nemty ransomware, SCULLY SPIDER's DanaBot, GRACEFUL SPIDER's GetAndGo Loader and the Latin America-targeted malware Kiron. There have also been instances of **eCrime actors attempting to sell COVID-19-themed tools**, including a phishing method using a payload preloader masked as a COVID-19 map.

Observed Activity: Targeted Intrusion

Despite the impact of COVID-19 on their respective countries, CrowdStrike Intelligence has observed multiple nation-state-affiliated targeted intrusion adversaries remaining active with spear-phishing campaigns throughout the last few months. Moreover, many of these adversaries have already been observed using COVID-19-themed operations: China-based PIRATE PANDA was observed using COVID-19-themed lure documents in February 2020; Democratic People's Republic of Korea (DPRK) adversary VELVET CHOLLIMA has also remained active and recently leveraged a COVID-19-themed lure document to deliver its unique BabyShark malware against South Korea-based organizations.

Tactic: Targeting Remote Services

It is possible that companies will increase the use of software as a service (SaaS) and cloud-based remote connectivity services in order to enable and support employees working from home. Standing up remote working services could pose a potential security risk when combined with possible human-error-enabled security lapses.

Criminal actors in particular continually seek to collect credentials for these services, potentially allowing them to gain access to these SaaS accounts and victim organization data. The eCrime big game hunting (BGH) ransomware industry in particular leverages Remote Desktop Protocol (RDP) brute forcing or password spraying for initial entry. As many sophisticated BGH actors remain highly active at present, they will likely attempt to capitalize on possible staffing disruptions COVID-19 may bring to organizations, as well as attempt to compromise employee devices while they work remotely.

Tactic: Vishing Robocall and Tech Support Scams

As employees shift to flexible work arrangements such as telecommuting, they will increasingly rely on phone communications to maintain and continue business operations. Adversaries are taking advantage of this situation to conduct malicious operations attempting to mimic official business communications. Such operations include voice phishing or "vishing" and robocall scams, as well as technical support scams.

Criminals have been observed using the COVID-19 outbreak as a theme in vishing and robocall scams. A portion of these calls initially focused on targets on the U.S. West Coast, as well as industries affected by the outbreak, such as transportation and travel. In some cases, vishing can be combined with smishing (text message phishing) in order to perpetrate such scams or load malicious content onto mobile devices.

Technical support scams use various delivery methods including phone calls, pop-up warnings and redirects. Although the theme of these scams may not be directly related to COVID-19, the increase in office workers transitioning to remote work in the near term poses the risk of increased tech support scams targeting those individuals, who may not be adept at or self-sufficient in remote computing.

Recommendations for Defending Against COVID-19 Scams

As the global COVID-19 outbreak grows, CrowdStrike assesses that malicious cyber threat actors will continue to take advantage of the situation. As such, it is imperative that businesses and employees remain aware of the potential cyber threats they face while they make transitions to alternative business continuity plans, and that they are informed of the immediate steps they can take to mitigate potential risks.

CrowdStrike recommends adopting a strong defensive posture by ensuring that remote services, VPNs and multifactor authentication solutions are fully patched and properly integrated, and by providing security awareness training for employees working from home.

For recent observed activity, see the Appendix at the end of this eBook.

Chapter 3
Getting the Most From Prevention Tools

by Senior Director of Product Marketing **Con Mallon**

As organizations deal with newly remote workers and business uncertainty, prevention is more important than ever. Cyberattackers are looking to capitalize on the current climate and seek vulnerabilities. The CrowdStrike Services team saw a record number of ransomware infections, data leaks and targeted attacks in 2019 — as well as a troubling trend: Organizations are often failing to enable key preventative features designed to stop malicious activity. Failure to configure these tools properly is often worse than not having them in the first place because it can give organizations a false sense of security and waste security budgets. While this is not a new phenomenon, the growing frequency of ransomware and other disruptive attacks is increasing the impact on organizations that fail to effectively block malicious activity.

Misconfigured Security Toolsets

It is not uncommon for the CrowdStrike Services team to encounter cutting-edge security toolsets that are not properly managed. This includes unpatched exploits, severe misconfigurations and botched deployments that can allow attackers to infect endpoints and move laterally throughout the environment. Large companies are not immune to this pitfall — in fact, CrowdStrike Services found that they are often more likely to not configure or misconfigure their security tools. Even though they have significantly more resources than smaller organizations, they often have sprawling footprints, complex networks and multiple improvement projects running at any given time, and they sometimes fail to dot all the i's and cross all the t's. This observation is troubling — due to current circumstances, the move to a more remote and dispersed workforce and operations is likely to exacerbate the problem.

This issue isn't limited to endpoint detection platforms. The team has also found crucial misconfigurations in intrusion prevention systems, data loss prevention tools, multi-factor authentication (MFA) platforms and cloud access security brokers. For example, the CrowdStrike Services team has responded to incidents where security controls — such as next-generation firewalls that segment corporate and production networks — were in place, but the victims had failed to configure any firewall rules. This allowed malware to quickly spread laterally to business-critical production equipment.

Maximizing Prevention Capabilities

Although misconfigurations are probably not significantly more common now than in years past, current threat trends place greater dependence on prevention, which makes misconfigured or under-optimized tools more problematic. And, like most human factors in security, it manifests in different ways. In some instances, security tools are deployed in "monitor" or "detect" mode during proof-of-concept testing to prevent disruptions in an environment, and more stringent prevention features are never enabled. In other cases, information security teams are requesting these features to be enabled, but IT teams are not responding, either because they do not trust the tool or it is not a priority. Even more troubling, some companies purchase security tools just to meet compliance requirements and never fully implement them, leading security teams to believe they are protected when they are not.

Because there is no single cause, there is no single fix. But there are steps that organizations can take to maximize the efficacy of their tools, both now and as good standard practice moving forward:

- **Never purchase a tool just for compliance reasons.** It is fine for compliance to be a driver in a technology purchase, but there must be people assigned to use and optimize the tools and processes.

- **Develop implementation plans for any new tools.** These plans should involve both IT and information security teams to ensure that stakeholders are aware of the tool's purpose and intended use. This planning process should also identify the tool's operational impact on the business and the degree to which that can be tolerated.

- **Establish change management guidelines.** A tool's agreed-upon configuration should be documented and then audited multiple times a year. Information security teams should frequently discuss configurations and new features with vendors and support teams to maximize the tool's value and validate its use in the organization's environment.

- **Develop a detection and prevention framework.** Not every tool needs to be deployed with the strictest preventative configurations enabled, especially if compensating controls exist. Implementing a detection and prevention framework should identify the threats and use cases that an organization wants to address, and also identify which tools are mapped to which use cases. This provides an excellent foundation for determining which use cases to prevent and which ones to detect, and with what tools. It also provides a great source of security metrics.

- **Test yourself.** Regular audits and adversary emulation exercises should ensure that the tools are working as intended.

- **Take a risk-based approach.** Ideally, organizations would tune their toolsets endlessly in pursuit of optimal security. This is great if you have the time and resources, but it's not feasible for most organizations. If you can't lock everything down, choose your battles. Identify the attacks you most want to prevent and focus on them first.

Chapter 4
Attackers Are Targeting Cloud Service Providers

by Senior Director of Product Marketing **Con Mallon**

The compromise of public cloud-based infrastructure is on the rise. Given current circumstances, organizations are looking to ensure they can continue to operate. This may require them to stand up new services and capabilities — and do so fast. The availability of public and private cloud infrastructure is an effective tool for organizations to accomplish this. In recent months, the CrowdStrike Services team has observed increasingly sophisticated operations in which financially motivated adversaries are using cloud application programming interface (API) keys to harvest information assets for ransom or sale. They are also often seeking other keys and passwords to facilitate further access, enabling them to repeat the cycle. And now, with many organizations increasingly moving their resources to the cloud and attackers looking to exploit any weaknesses, cloud security must be a top priority.

New Attack Surfaces

Internet-as-a-service (IaaS) API key theft has opened a vast new attack surface, giving adversaries easy access to critical controls and data assets when appropriate protection is not in place. As discussed in the latest **CrowdStrike Services Cyber Front Lines Report**, many recent cases have involved static credentials that were not protected by MFA, IP address-based restrictions or automatic rotation. Previously, when threat actors harvested API keys from public source code repositories, it was typically a crime of opportunity. Now, it's become targeted, and CrowdStrike has responded to multiple cases in which attackers actively sought cloud IaaS API keys in client and third-party infrastructure. In virtually all cases, these long-lived API keys were an unnecessary liability as they could have been replaced with ephemeral credentials issued through the underlying cloud infrastructure.

Detection Time Is Key

In addition, detection times can range from hours to months, and in many cases, data exfiltration has occurred before detection. Host-level compromise in the cloud continues, and many cases involve "shadow IT" cloud deployments — deployments that receive limited security oversight and investment. The Services team has observed gaps in endpoint (instance/VM) detection capabilities, misconfigured logging, misconfigured firewall rules, and lack of system and application vulnerability management.

In some cases, security staff were already stretched thin in their efforts to secure on-premises resources, or they lacked familiarity and experience with cloud environments. In others, serious incidents affected infrastructure that was already slated to be decommissioned prior to compromise. The Services team considers these trends a contributing factor in compromises resulting from both nation-state and financially motivated operations.

CrowdStrike continues to recommend the following practices to help organizations prevent breaches of their cloud infrastructure:

Avoid using static API keys anywhere. Static keys pose a significant risk because they allow enduring access to large amounts of often-sensitive data. Instead, use ephemeral credentials for automated cloud activity and enforce the usage of these credentials only from authorized IP address space. Also, require MFA for all user-originated cloud activity.

Proactively manage cloud accounts and permissions. Begin this process by conducting an account inventory to ensure every resource has an identified owner/responsible party. Next, use a cloud account factory model to ensure new cloud accounts comply with security expectations from the start. You should also review permissions in legacy or to-be-decommissioned cloud accounts for excessive public access to hosts and storage services. Finally, find cloud accounts/subscriptions that are not being monitored by looking for references to unrecognized cloud accounts. This can be achieved by collaborating with the finance department to find unrecognized cloud subscriptions.

Enable logging and alerting. Enable detailed logging, including API and data object access logging, to the maximum extent affordable. Also, invest in and tune automated alerting to rapidly identify incidents and revert improper configuration changes.

Regularly review firewall rules on the cloud. Use automated and manual firewall ruleset reviews to avoid global-permit rules in both inbound and outbound contexts.

Chapter 5
Vulnerability Management with a Distributed Workforce

by Product Marketing Director **Scott Taschler**

Maintaining an accurate, up-to-date picture of organizational risk becomes increasingly important as workers move from traditional offices to work-from-home environments. Laptops leaving the safety of the office security perimeter often have sensitive information and provide users with access to critical systems.

Organizations need to maintain a clear understanding of the security posture of these systems, regardless of where they are located. When a critical vulnerability is disclosed, the race is on to reduce the attack surface before an exploit becomes widespread. In these situations, assessing your exposure to new threats in real time can be critical, but is often not possible for work-from-home users.

Challenges Scanning Remote Systems

Vulnerability management requires a different approach in a work-from-home world. The systems and processes that many organizations have developed over the years to assess and manage vulnerabilities are based on the premise that users are primarily working from an office. These systems leverage network-based scanning appliances to run recurring scans that identify what systems are on the network, and to assess what patches are installed as well as what other vulnerabilities may be present on these systems.

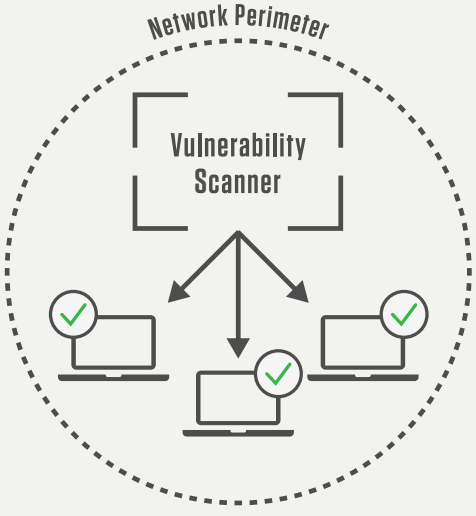

Figure 1. Vulnerability Assessment On-premises

When your users are working from machines that are no longer located in an office with a high-bandwidth corporate LAN (local area network), network-based vulnerability scanning is no longer a feasible option. In the best-case scenario, remote users connect to the office via VPN. In these cases, it may be technically possible to scan systems over the VPN tunnel, but scanning eats up limited network bandwidth that must be conserved for business activity. This makes network-based vulnerability scanning highly impractical for VPN-connected users.

In other cases, work-from-home users may be primarily using cloud-based services that do not require a direct connection to the corporate network. This renders network-based vulnerability scanning completely ineffective.

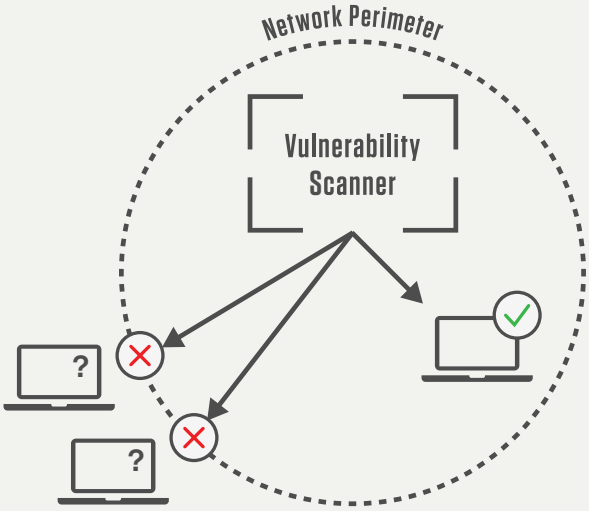

Figure 2. Vulnerability Assessment Off-premises

When workers are operating from home offices for weeks or months on end, it creates massive blind spots for IT security staff. This introduces unknown risks to the organization and can slow down efforts to remediate critical threats.

A Step in the Right Direction: Agent-based Vulnerability Assessment

Some vulnerability assessment solutions leverage local agents installed on individual endpoints to address this visibility gap. Performing vulnerability assessment on the host itself can solve the problem of how to execute the assessment, as it does not require a network-based appliance to communicate with the endpoints. However, it also introduces additional challenges for over-taxed IT staff.

For starters, installing an additional agent for vulnerability assessment introduces complexity and consumes system resources. This can be particularly troublesome to deal with when users don't have access to local IT staff to help with installation and resolution of problems. In addition, if users are not connected to the corporate LAN via VPN or other means, it may be impossible for IT security staff to collect and analyze results of agent-based scans in a timely manner.

Cloud-native, Scanless Vulnerability Assessment Fills the Gap

With users essentially working from the cloud, it makes sense to tap into the power of the cloud to provide them protection. The CrowdStrike Falcon platform was built from the ground up to meet these challenges.

The cloud-native Falcon platform leverages a single lightweight agent to seamlessly collect security telemetry from systems wherever they reside: on-premises, off-premises or in the cloud. This not only provides organizations with best-in-class endpoint protection but also deep visibility into vulnerabilities, via the Falcon Spotlight™ module. Falcon Spotlight ensures that defenders always have a real-time picture of the security posture of their assets, ensuring fast detection of threats, regardless of geography and without deploying additional agents or impacting endpoint performance.

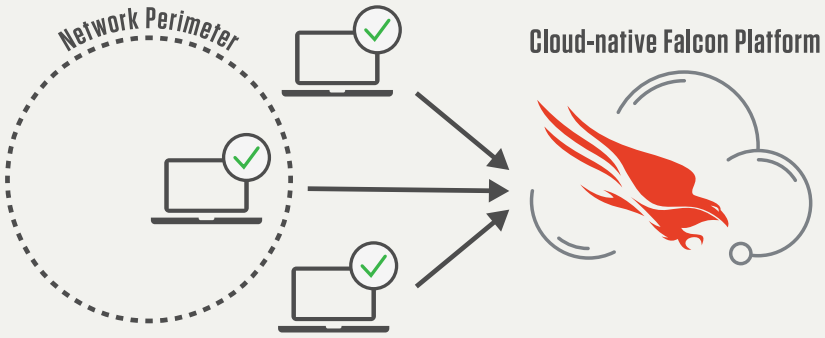

Figure 3. Cloud-native, Scanless Vulnerability Assessment

Changes in work habits mean re-evaluating defenses to ensure that they continue to provide the protection, visibility and response capabilities that organizations need to keep users and data safe. CrowdStrike's cloud-native solutions allow organizations to pivot seamlessly across the full range of potential work models without sacrificing security or performance.

Chapter 6
New Emphasis on an Old Problem: Patch Management and Accountability

by Senior Director of Product Marketing **Con Mallon**

Vulnerability and patch management is a decades-old cybersecurity problem, and given the current worldwide pandemic and how **nation-state and eCrime adversaries** are exploiting it, mitigating vulnerabilities across your organization's environment has never been more important — especially as increasing numbers of remote employees are connecting their personal devices to corporate networks. Traditionally, discovering and finding vulnerabilities would become harder when you had many users working remotely. It required organizations to "scan" for vulnerabilities on their endpoints, and this task was made harder if that endpoint was not connected to the network or operating beyond the corporate firewall. It could take hours, days or even weeks to gather results. Fortunately, with approaches such as CrowdStrike Falcon Spotlight vulnerability management, organizations have visibility into the vulnerabilities on their endpoints and environment in real time, without the need to scan.

The CrowdStrike Services team has observed many organizations still struggling to identify vulnerabilities, prioritize critical systems and deploy patches, as covered in the recently released **CrowdStrike Services Cyber Front Lines Report**. As a result, many companies have continued to suffer from **ransomware attacks** and **malware** that leverage exploit kits designed to prey on vulnerabilities in unpatched systems.

Organizations often experience vulnerability and patching issues because of departmental conflicts, missing patch management policies and limited accountability. Fortunately, many companies are developing new, risk-based solutions that can be highly effective in addressing the persistent challenges that patching presents.

Problem 1: Vulnerabilities Everywhere, Patches Nowhere

Information security teams often have a lot of data on the vulnerabilities in their environments, but they usually rely on IT teams to test and deploy patches. This is one area where organizations frequently fail. Information security teams and IT teams often have competing priorities — information security wants to keep an organization's critical systems safe, while IT wants to keep them working. And for a small or medium-sized business (SMB), information security and IT might be the responsibility of the same person. If patching becomes a low priority, it can eventually cost the business money.

Problem 2: Just Patch Everything

When information security teams approach IT departments with lists of systems to patch, it's often overwhelming, and prioritization can be a challenge. The IT team may want to patch an internet-facing email server first — since it contains information about the organization's trade secrets and has a high risk of attack — and hold off on critical patches to VPN software because of difficult deployment procedures and potential

business interruptions. But the information security team may have threat intelligence reports showing that adversaries are actively exploiting the organization's VPN vulnerabilities. For SMBs with a small team, patching everything is often not feasible, and determining where to focus limited resources adds further complication.

Problem 3: No One Will Notice

CrowdStrike Services commonly sees a lack of accountability for failing to implement patches. Most organizations don't have formal patching policies or enforcement mechanisms to ensure their systems stay patched, and incentives for information security and IT teams are often lacking. Pushing out patches isn't exciting work, and these tasks frequently get moved to the bottom of the project list. While automation can help, applying critical patches to equipment or systems that require around-the-clock uptime requires maintenance windows and significant resources — and technology teams can too easily forego these tasks in the name of business continuity, without experiencing any immediate ramifications.

What You Can Do

Fortunately, many companies are developing new, risk-based solutions that can be highly effective in addressing the persistent challenges that patching presents. CrowdStrike recommends the following practices for patch management and accountability to keep your organization safe, both now and once the current health crisis has passed:

Leverage a risk-assessment framework. Most organizations don't treat vulnerability risk with the same seriousness as other enterprise risks. Organizations need vulnerability management and patching policies that define service-level agreements for both information security and IT teams, and both teams need to work together to define the systems they consider most critical. Then teams can create a priority list that shows what should be patched first and what operational risks are being taken for each system.

Use documentation to drive accountability. Information security and IT managers need to document why they are choosing to address specific vulnerabilities or patches but not others. The executive team should be responsible for signing off on the exceptions, validating that the organization is choosing to accept the risk. This hierarchy of vulnerability management can keep teams accountable and ensure that systems are patched in a timely manner.

Create a dedicated vulnerability management team. For organizations with sufficient resources, CrowdStrike recommends dedicating information security and IT personnel to vulnerability and patch management. This team is then accountable for identifying vulnerabilities and deploying patches quickly, guided by the risk-assessment framework described above. The key advantage is that information security leaders can produce metrics to assess the effectiveness of the program. Based on these metrics, the executive team may decide to increase investment in vulnerability and patch management.

Deploy patch prioritization and automation tools. Tools are available to assist and enhance how organizations operationalize patching efforts. Patch prioritization helps organizations make better decisions to reduce IT security risk, while patch automation solutions can dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation. Patch prioritization and automation applications are available in the **CrowdStrike Store**.

Chapter 7
Remote Incident Response and Endpoint Recovery

by Senior Manager of Product Marketing **Paul Ashwood**

It's clear that cybercrime and cybercriminals are not letting up during the global upheaval caused by COVID-19. In addition to the many problems organizations are facing in having to rapidly enable a remote workforce, the global pandemic presents a challenge in how organizations will detect, respond to and recover from a cyber incident. What happens when **nation-state and eCrime adversaries** exploit a vulnerability and you need to engage an incident response (IR) team, but the team is unable to travel to the affected endpoints? Here are some of the issues organizations could encounter:

- With a newly remote workforce, the perimeter to secure and monitor has now grown substantially
- Physical access to systems and endpoints is now limited or even prohibited
- The ability to perform remote host recovery and remediation is critical to sustainable operations
- Security teams and incident workflows are now decentralized
- There is a limited or non-existent ability to collect, analyze and remediate endpoints remotely
- Handling endpoint updates and management can be challenging, and on-premises access may be required

The ability of an IR team to perform response, recovery and remediation actions remotely is essential in the face of attack. With the number of phishing scams surrounding the COVID-19 pandemic on the rise and more employees working remotely on unprotected home computers and other devices, the risk of an attack is greatly increased.

Organizations should be looking at their IR plans and talking with their IR teams to understand needs and capabilities, decide what work can be performed from remote locations, and determine risks due to any need to be on-site, with physical access to systems.

Most IR engagements begin by deploying the tools necessary to gather the intelligence and digital forensics required to investigate an incident and gain immediate visibility into the active threat that caused the breach. If your current IR plan requires a hardware solution to be shipped and installed on-site — including configuring the software — just to get started, then a traditional approach to remediation becomes even more problematic, given limited or prohibited access to the data center.

Response

Rapid response begins with the technical components of an IR solution being deployed remotely. The cloud-native architecture of the CrowdStrike Falcon platform enables CrowdStrike to remotely deploy the Falcon agent to thousands of endpoints within hours of starting an IR engagement. There is no requirement to ship hardware to a location — you simply deploy the Falcon agent remotely to gather the telemetry that will give the IR team immediate visibility into the active threat context.

In addition, CrowdStrike incident responders will remotely use the Falcon Forensics Collector (FFC) to preserve the historical digital forensic information needed to fully investigate an incident — gaining an understanding of "who, what, where, when and why" a nation-state or eCrime adversary has exploited a vulnerability and breached the network.

Using the current attack vectors gained from the Falcon agent and the historical activity from log files and other forensically significant artifacts, the IR team now has full visibility into the attack context as part of the incident triage within minutes of deploying the Falcon solution.

Recovery

At this point in the process, the emphasis is on rapid recovery of endpoints so that normal operations can proceed with minimal effect on users and zero business impact. Once having gained visibility across the current attack — investigating the adversary conducting the attack; the tactics, techniques and procedures (TTPs) being used; and the affected endpoints or hosts — the IR team is now in a position to begin surgically removing the threat from the endpoints.

Traditional IR relies heavily on machine reimaging to solve this problem. Reimaging a large number of endpoints is extremely inefficient. It is not only very disruptive for end users, it usually requires an on-site presence to handle multiple system reboots — and generally, this is quite disruptive to the business. In addition, there is no guarantee that the last known image, which is being restored, is a good image. This inability to perform remote host recovery and remediation can significantly extend the time it takes to recover from an incident.

Fortunately, there is a better way to recover. There are tools and approaches for remotely connecting to an endpoint, removing any malware and reconfiguring protection to ensure there is no recurrence of the attack or intrusion. However, it requires the skill and experience of a responder to effectively and efficiently use these tools. Using the Falcon platform Real-Time Response (RTR) functionality enables the CrowdStrike IR team to surgically remove threats from endpoint devices with speed and precision. Falcon RTR enables the team to remotely kill processes, delete files, modify registry entries, execute scripts and ultimately recover the endpoint by removing advanced persistent threats without the need to reimage the machine. Based on the known TTPs identified in the response phase of the engagement, the CrowdStrike IR team uses its playbooks to recover endpoints, using RTR to access the host devices from anywhere in the world and execute the commands needed to surgically remove a threat and restore the endpoint — with no reimaging, no rebooting and no disruption to the end-user device.

Remediation

With the threat identified, affected machines isolated and endpoints recovered, the IR team then turns its attention to the exploit that was used to gain access. The goal is to ensure that the vulnerability is remediated and further breaches are prevented. Remediation often involves patch management requests to the IT department to patch a server or firewall and may require modifying certain workflows and access rights in order to close down the vulnerability. These actions take time and coordination, so it is important to maintain the highest level of diligence, with continued threat hunting on a 24/7 basis for the remainder of the IR engagement.

Once an adversary has breached a network, they will keep coming back — believing the organization is an easy target for more attacks. That's why it is so important to continuously monitor the environment for security threats using advanced threat hunting to detect, investigate and remediate any further attacks and truly stop breaches.

At this point, organizations may consider moving or bolstering their cybersecurity efforts by having endpoint protection delivered as a fully managed service such as CrowdStrike Falcon Complete. This worry-free solution allows customers to entrust the implementation, management and incident response of their endpoint security to CrowdStrike's proven team of security experts. The result is an instantly optimized security posture without the burden, overhead and cost of internally managing a comprehensive endpoint security program. CrowdStrike Falcon Complete uniquely provides the technology, platform, actionable intelligence and skilled expertise required to ensure comprehensive endpoint security from beginning to end.

And, one final consideration: If the transition to employees working from home means they will be using various personal devices, it is a good idea to scan your network for basic IT hygiene, such as identifying unprotected endpoints that may be on the network. Unprotected endpoints will no doubt be the ideal vulnerability used for the next wave of attacks.

Chapter 8
How CrowdStrike Store Partners Are Helping to Secure Remote Workforces

by VP of CrowdStrike Store Business **Andy Horwitz**

As CrowdStrike continues to provide practical guidance and resources for customers, it is bolstered and supported by the CrowdStrike Store partners, who are also guiding and assisting organizations as they transition to a more remote operations model. If you are interested in leveraging any of the special offers or programs provided by CrowdStrike Store partners or participating in free trials of our applications, visit **the CrowdStrike Store webpage** and learn how to become a Store customer.

The following are just a few examples of Store partners that are providing valuable assistance during this difficult time by extending special offers on applications that help organizations enhance protection for remote workers.

Reducing Exposure with Vulnerability Risk Management

NopSec Unified VRM® (Vulnerability Risk Management): This application ingests vulnerabilities uncovered by the CrowdStrike Falcon platform and provides contextual enrichment and deeper insight into overall risk exposure. Having visibility into existing risks from vulnerabilities and risk prioritization helps reduce the time to remediation for critical security gaps and improve security posture across your organization.

Organizations are increasingly setting up remote working systems, such as virtual desktop infrastructure (VDI) servers, remote desktop connections and others, to support employees working from home. That's why it's essential to have a robust vulnerability and security configuration management plan in place to help protect against security gaps in new remote work systems that can be leveraged by adversaries. To assist customers during the crisis, NopSec is providing a special discounted COVID-19 offer on its Unified VRM solution. This offer includes three months of NopSec Unified VRM to help assess vulnerabilities for internet-facing assets and aid organizations in protecting their remote workforces and digital footprints. Read more about the offer on this webpage: **Empowering Remote Workforce During COVID-19**.

Hardening Remote User Endpoints

Automox: This app empowers customers to act on any vulnerability discovered by the CrowdStrike Falcon platform, and it proactively eliminates exposure before those vulnerabilities can be weaponized. The app works by enabling patch deployment via real-time visibility into the patch status of all remote endpoints in the customer's environment.

With new remote systems getting spun up quickly to provide access to corporate assets and data, it is imperative that all vulnerabilities be monitored, prioritized and patched before they become sources of a breach.To cope with the rapid transitions caused by COVID-19, Automox is now offering a 90-day, extended free trial of its endpoint hardening and patch management solution to protect remote endpoints against existing vulnerabilities before they can be compromised. This offer provides full service and support for an unlimited number of endpoints, without the need for VPNs or corporate network connectivity. Learn more about it in this Automax blog: **Supporting Remote Work During COVID-19**.

Deeper Defense with Digital Attack Surface Management

RiskIQ Illuminate: This app combines CrowdStrike's endpoint telemetry with RiskIQ's comprehensive internet data to provide a 360-degree view of customers' digital attack surfaces, allowing them to better detect threats and defend their organizations.

Security teams and analysts are facing unprecedented threats and adversary attacks, compounded by the fact that they have to support a dispersed workforce and business operations that were previously restricted within the organization's corporate IT infrastructure. To help the security community defend against emerging threats, RiskIQ is providing 30-day research access to PassiveTotal, its solution for expediting the process by which analysts investigate threats and respond to incidents. RiskIQ will also provide daily threat infrastructure lists that match specific terms related to the COVID-19 pandemic, as well as a free Digital Footprint Snapshot Report to help customers understand how their attack surface is expanding. Learn more about it in this RiskIQ blog: **Discovering Unknowns and Investigating Threats Amid a Global Pandemic**.

Protecting Collaboration Platforms

SafeGuard Cyber: This app works with the CrowdStrike Falcon platform to extend visibility of detected threat activities occurring on protected accounts across 50-plus social, mobile and collaboration channels. This includes social platforms such as Facebook, Twitter, Microsoft Teams, LinkedIn, Slack and Salesforce.

Since the outbreak, more and more companies are adopting collaboration software to ensure business continuity and are also using expanded feature sets in existing tools. With communication and new software platforms on the rise and workplaces becoming more digital, new threats from both external and internal sources are increasing. SafeGuard Cyber is offering 60 days of free collaboration security software for companies to protect their remote users and data across a number of commonly used collaboration software platforms. With the use of collaboration tools on the rise, it is critical to protect against threats including phishing and vishing attacks. Read more about it in this SafeGuard blog: **COVID-19 (Coronavirus): Scaling Security for Remote Workforce Demands**.

Securing Remote Access for ICS Environments

Dragos: This app provides visibility into and early warning of threats in industrial control systems (ICS) and operational technology (OT) environments by leveraging endpoint data collected by the CrowdStrike Falcon platform. This capability reduces the risk of disrupting business operations by stopping threats before they can pivot into vital ICS/OT systems.

With the changing threat landscape and the current COVID-19 crisis, organizations with ICS and OT environments have been forced to transition quickly from traditional on-site support to remote support access. This requires adding digital connectivity across remote ICS/OT sites to allow workforces to access them from locations other than on-premises. With expanded remote access, securing ICS/OT systems, improving monitoring and visibility, and using rigorous security controls become critical factors in effectively protecting against industrial threat adversaries. Read more about the best practices Dragos recommends in this blog: **A Matter of Trust: Remote Access for ICS**.

"Better Together" Cybersecurity Programs

CrowdStrike and its Store partners are working together to empower customers to defend against advanced threats during this period of uncertainty and challenging circumstances. Organizations need to remain nimble in order to react quickly to updated recommendations and mandates from authorities without compromising their own security. The CrowdStrike Store is a clear example of adherence to the "one team, one fight" maxim, where CrowdStrike joins together with its partners to ensure customers are better protected from cybercrime and cybercriminals.

Chapter 9
COVID-19 Cybersecurity Challenges and Recommendations

by CTO **Mike Sentonas**

CrowdStrike's on-demand webcast, "**Cybersecurity in the Time of COVID-19**," discusses ways for companies to overcome the cybersecurity challenges they're facing during this worldwide crisis, and provides suggestions for how to make a smoother and more secure transition to a remote workforce. If the following key factors aren't already a part of your security strategy, they should be part of your planning going forward:

Have comprehensive cybersecurity policies in place. Organizations that haven't had a remote workforce enabled may not have policies in place that cover all the factors involved. Employees may be connecting from a variety of personal devices — laptops, tablets, Android and iPhone — so you must have policies that encompass all contingencies, whether employees are on corporate-owned or personal devices.

Ensure adherence to compliance and privacy issues. You need to consider the privacy of employees working on personal devices as well as the data that may now be accessed from those personally owned devices. It's important to understand how General Data Protection Regulation (GDPR) and other compliance regulations impact your remote workforce, and ensure that your employees are aware of the compliance requirements governing your organization's data.

Cybersecurity hygiene and visibility are critical. To have adequate cybersecurity, you need to adopt a "hygiene first" approach that will give you full visibility into your IT environment and help you address blind spots in your architecture. This is especially true with a newly deployed remote workforce. Make sure you know the "who, what and where" of your environment: who is on the network, what apps are being used and where you may need to address security gaps.

Plan for patching remote systems at scale. User laptops may remain out of the office for weeks or months to come. Patch management systems are bandwidth-hungry applications and may not scale well for hundreds or thousands of users on the other side of a VPN. New vulnerabilities are sure to be announced in the coming weeks, and adversaries understand that the tools and processes you use to patch them are likely to be operating at reduced effectiveness. Fast and effective patching remains one of the most critical methods for blocking attacks at the earliest stages.

Continued education is a must as COVID-19-themed scams escalate. As long as the COVID-19 outbreak continues, malicious cyber threat actors will continue to take advantage of the situation with coronavirus-themed phishing attacks and scam campaigns. It is imperative that businesses provide continuous security awareness training to ensure employees remain mindful of these threats. Organizations should also adopt a strong defensive posture by ensuring that remote services, VPNs and multi-factor authentication solutions are fully patched and properly integrated.

Crisis management and incident response plans need to be executable by a remote workforce. Effective remote collaboration tools — including conference bridges, instant messaging platforms and productivity applications — can allow a dispersed team to create a "virtual war room" from which to manage remediation and response efforts.

Ensure you can respond, recover and remediate remotely. Attacks and intrusions are not going to stop, and you need to ensure you have the resources and capabilities to respond remotely and protect your organization. Incident response, endpoint recovery and remediation can and will need to be undertaken remotely. Understanding this requirement can help inform the decisions you make in preparation.

Protect remote endpoints with an effective endpoint protection solution. Employees working from home are either using company-issued devices or their personal systems. Those devices and systems need to be protected because they constitute a gateway to corporate networks and resources. In addition, a laptop or desktop used for both private and professional purposes is potentially exposed to more risks than an IT-controlled corporate device. The chosen solution should be remotely deployable and manageable, should not impact end user performance, should prevent malware and ransomware, and should provide protection against sophisticated malware-free, nation-state-sponsored attacks.

About CrowdStrike

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: **We stop breaches.**

Appendix
Recently Observed Cyber Threat Activity

Adversaries continue to use social engineering techniques and malicious documents referring to Coronavirus Disease 2019 (COVID-19). Since mid-March, CrowdStrike® Intelligence has made public the following notable threats using COVID-19 themes. These activities are also **updated weekly in the COVID-19 Cyber Threats intel blog**.

Observed Activity Update: April 13 to April 20, 2020

- eCrime actors continue to use social engineering techniques and malicious documents referring to COVID-19. Impersonation of the World Health Organization (WHO) remains a popular social engineering technique in phishing campaigns. CrowdStrike Intelligence recently observed a new campaign that used a spoof sender address (WHO <eurohealthycities@who[.]int>). The emails delivered the "AgentTesla" information stealer using an exploit document known as "Virgo." AgentTesla has been one of the most popular final payloads delivered by eCrime adversaries using COVID-19-related lures. WHO did not send these emails, please read this security alert [who.int] for more information.
- On April 14, 2020, CrowdStrike Intelligence observed a spam campaign distributing Hancitor using a COVID-19-themed lure and Microsoft Excel 4.0 macro documents. The emails purported to be an "invoice message" related to a recent purchase of a COVID-19 protection plan with a link providing additional details. While this is not the first time Hancitor operators have been observed using a COVID-19-themed lure, it is the first time Excel 4.0 macro documents have been used. Similar to past campaigns, Hancitor continues to download final payloads of Pony and CRE Stealer.

  A new malicious Microsoft Office Word document was identified:

```
ООН пообещала помощь Кыргызстану в борьбе с коронавирусом.rtf
```

  The translation is: "UN promised assistance to Kyrgyzstan in the fight against coronavirus.rtf." This file displays Russian-language decoy content related to the Kyrgyzstan government's response to the global COVID-19 pandemic, copied from an April 6, 2020, press release posted on the official government of Kyrgyzstan website www.president[.]kg. This document delivers the Chinozy malware associated with an activity cluster tracked by CrowdStrike as StrangeVantage. Similar StrangeVantage activity has been observed by CrowdStrike Intelligence as recently as mid-March 2020. While this activity cluster is currently unattributed, it is assessed with moderate confidence as likely to be associated with China-nexus targeted intrusion operations.

Observed Activity Update: April 6 to April 13, 2020

- On April 9, 2020, CrowdStrike Intelligence identified a phishing email using the spoofed sender alias WHO <eurohealthycities@who[.]int>, referring to the WHO, which contained the subject "URGENT COVID-19 SUSPECTED AFFECTED VSL." The World Health Organization (WHO) did not send this email — please read this **security alert [who.int]** for more information.

  The message contained two malicious attachments: a Microsoft Excel workbook named COVID 19 MEASURES.xlsm, and a Microsoft Office document named DOCX.doc. DOCX.doc is a Virgo exploit document that exploits CVE-2017-0199 to run an embedded scriplet file. COVID 19 MEASURES.xlsm contains Visual Basic for Applications (VBA) macro code, which when enabled also downloads and runs a file. Both attachments download the same resource, http[:]//93.126.60[.]106/vDBAExRNFm.exe, which is the AgentTesla information stealer.

- CrowdStrike Intelligence has recently observed an unattributed targeted intrusion activity cluster using Coronavirus 2019 (COVID-19) and Southeast Asia-focused lures and themes to distribute the Chinoxy malware implant in March 2020. This activity is tracked by CrowdStrike Intelligence under the StrangeVantage activity cluster; while currently unattributed, CrowdStrike Intelligence assesses with moderate confidence that the StrangeVantage activity cluster is likely associated with Chinese-nexus targeted intrusion operations.

  On March 17, 2020, the malicious document "President discusses budget savings due to coronavirus with Finance Minister.rtf" was submitted to a third-party virus scanning service. Following this submission, several malicious documents with Malaysian-language government decoy and lure content were also identified. While all three documents use vulnerabilities in the Microsoft Equation editor to deploy the Chinoxy implant, there are slight differences in execution and persistence mechanisms.

- CrowdStrike Intelligence has identified incidents involving the likely malicious use of a publicly available penetration testing tool named Octopus. This tool is available on GitHub and is intended for use in legitimate red team operations. Octopus is a modular tool and includes functionality that allows users to carry out a range of actions on a victim machine. Identified incidents indicate malicious actors have likely been using Octopus since at least early 2020. CrowdStrike assesses it is highly likely this tool will continue to be used in malicious activity due to its public availability and functionality.

  Follow-on research into malicious incidents using Octopus led CrowdStrike Intelligence to identify an Octopus PowerShell agent linked to network infrastructure associated with other malicious files. This Octopus agent was configured to communicate with the C2 IP address 212.71.248[.]46. This IP address has also served as a C2 for two other files: a Microsoft Word document with malicious macros and a malicious executable which has yet to be identified. The malicious document is named COVID-19 SAFETY TIPS.docm and contains a PowerShell Empire-based malicious macro.|

- On March 26, 2020, public reporting identified multiple Coronavirus Disease 2019 (COVID-19)-themed mobile threats targeting Android-based mobile users. CrowdStrike Intelligence has analyzed a number of these threats, including AdoBot and Cerberus, which aim to take advantage of the COVID-19 pandemic.

- At the beginning of April 2020, a hospitality organization operating in the Middle East received an email with the subject line "Pak Army Deployed in Country in Fight Against Coronavirus." The email body contained spoofed information regarding a fictitious government decision to nationally deploy the Pakistani army among broader efforts to control the spread of the COVID-19 virus. Due to thematic and tooling overlaps as well as common network infrastructure used, CrowdStrike Intelligence attributes this recent compromise attempt to the India-nexus BandRacer activity cluster with high confidence. Although BandRacer activity was consistently observed in 2018 and 2019, this incident is the first to be identified in 2020. This is also the first observed BandRacer incident targeting the hospitality sector; a significant portion of previously observed activity was assessed to be focused on government and military-related entities in Pakistan and China.

Observed Activity: March 30 to April 6, 2020

- A COVID-19-themed phishing campaign with the subject "COVID-19 UPDATE !!" was sent to victims, purportedly from the World Health Organization (WHO), with a malicious attachment named "Covid-19_UPDATE_PDF.7z." The 7-zip archive contained an executable sample of the information stealing malware LokiBot (CSIT-17123). WHO did not send this email; please read this **security alert** for more information.
- On March 30, 2020, an unattributed adversary sent a phishing message using the spoofed sender alias CDC Health Alert, referring to the U.S. Centers for Disease Control and Prevention (CDC), which contained the subject "CDC-INFO-Corona Virus Viccine found." The message included an attached Gzip archive named "Covid-19 Vaccine.gz." This archive contains the commodity NanoCore RAT, which is widely available in the criminal underground.
- On March 31, 2020, CrowdStrike Intelligence identified a second email impersonating the CDC to deliver NanoCore. The message body was apparently derived from a publication on the official CDC website. Instead of leveraging an attachment to deliver NanoCore, this email prompts recipients to "download the Vaccine" from a Microsoft OneDrive link. The message body additionally advises victims to contact a UK phone number if needed: "If you have more question please sms or Whatsapp me on: [UK phone number] on how to use the Vaccine." The use of a contact number is not common in criminal spam campaigns.
- A lure website referencing COVID-19 (masry-corona[.]com) was identified in use during March 2020 by distributors of the Culebra Variant information stealer to attract internet visitors. The malware is commonly used to capture Latin America-based banking customers' credentials.
- AgentTesla continued its capitalization on the COVID-19 pandemic by distributing a spam campaign purportedly from Group Life and Health with the subject "Important Notice to Our Corporate Clients & Partners - COVID -19." The spam email contained the RAR archive attachment named "COVID-19 Communication to corporate Clients..rar." The archive file contained an executable file named "COVID-19 Communication to corporate Clients..exe." This executable is a sample of AgentTesla that communicates with the command-and-control (C2) server rajalakshmi[.]co.in.
- CrowdStrike Intelligence has obtained several Korean-language exploit documents themed with information pertaining to the COVID-19 pandemic in the Republic of Korea (ROK). Upon execution, these documents attempt to deliver two previously unobserved payloads. The exploit used in this activity and the targeting of individuals likely in the ROK is congruent with previously observed Democratic People's Republic of Korea (DPRK) operations; however, the payloads do not have any direct technical overlaps

with tools used by any tracked DPRK adversaries. CrowdStrike Intelligence assesses with moderate confidence that it is likely these exploit documents were deployed by a DPRK-aligned group, but does not attribute this new activity to a named adversary at the time of this writing.

Observed Activity: March 23 to March 30, 2020

- CrowdStrike Intelligence identified scam emails spoofing the **World Health Organization** (WHO) with requests for financial donations to the COVID-19 Solidarity Relief Fund. The emails copy legitimate communications from WHO regarding the fund, but list an adversary-controlled Bitcoin (BTC) wallet address for payment. The World Health Organization (WHO) did not send this email, please read this **security alert [who.int]** for more information.
- A malicious website (corona-virus-map[.]net) posing as a COVID-19 map was identified dropping SCULLY SPIDER's DanaBot banking trojan. The web inject primarily targeted U.S.-based financial institutions.
- On March 23, 2020, CrowdStrike Intelligence obtained a phishing message impersonating a U.S. government agency and using the subject line "COVID-19 – nCoV – Special Update – WHO." The message contained an attachment named "covid-19 – ncov – special update.doc." When opened, this file exploits a vulnerability in Microsoft Equation Editor and subsequently issues a GET request to download a file located at http[:]//getegroup[.]com/file.exe that leads to a WarZone remote access tool (RAT) sample. This malware uses phantom101.duckdns[.]org for command and control. WarZone is a commercially available RAT commonly used by cybercriminals.
- On March 23, 2020, a COVID-19-themed DNS hijacking campaign was identified that reportedly attempts to trick users into downloading Oski Stealer. By altering the DNS settings for D-Link and Linksys routers, users are directed to an actor-controlled site that claims WHO has released a COVID-19 information application.
- Compromised versions of an Android application called "SM_Covid19" are being distributed to unsuspecting users. The hijacked versions allow for the download and execution of additional malicious code on a user's device. The original app was developed by an Italy-based company to assist with applying social-distancing protocols during the COVID-19 pandemic.
- CrowdStrike Intelligence identified a malicious Microsoft Office exploit document with Mongolian-language lure content uploaded to a third-party file-scanning service. When opened, the document displays decoy content bearing Mongolian Ministry of Foreign Affairs (MFA) letterhead, related to a COVID-19 press release by the People's Republic of China (PRC). CrowdStrike Intelligence currently assesses there is an even chance this activity is associated with the KARMA PANDA (aka MysticChess) adversary. Further retrospective analysis has also identified suspected KARMA PANDA activity as early as December 2019.
- CrowdStrike Intelligence identified a COVID-19-themed lure document being used by VELVET CHOLLIMA to deliver its Konni implant. The file, titled "Keep an eye on North Korean cyber.doc," uses macros in an attempt to contact C2 infrastructure. VELVET CHOLLIMA has used COVID-19-themed documents several times over the past few weeks and is likely taking advantage of this significant geopolitical event to entice its targets to open malicious documents and execute its malware..

Observed Activity: March 16 to March 23, 2020

- On March 23, 2020, public reporting announced that some European-based hospitals had fallen victim to a Netwalker ransomware (aka KazKavKovKiz, Mailto, Mailto2 and KoKo) incident. The incident reportedly began on March 22, 2020, and used Coronavirus Disease 2019 (COVID-19) lures.
- Throughout March 2020, the RedLine information stealer has used COVID-19-themed spam purportedly originating from a project that simulates potential cures for diseases to evaluate their effectiveness.
- A new TrickBot dynamic web inject was distributed targeting customers of Italy-based financial institutions. It is highly likely that this is a continuation of efforts by WIZARD SPIDER to capitalize on COVID-19 — the group has used COVID-19-themed lures during distribution. The new dynamic web inject is likely seeking to exploit the inevitable increase in online banking by Italian users during the current lockdown conditions.
- On March 16, 2020, the Australian Cyber Security Centre (ACSC) **reported** a text phishing scam claiming to offer advice on local COVID-19 testing facilities. Interacting with the URL within the text dropped the commodity banking trojan Cerberus via a malicious Android application package.
- A Nemty ransomware (v2.6) sample was detected on March 18, 2020, targeting a government entity. The lure email spoofed the chief executive office of a healthcare organization and referenced an annual general meeting purportedly scheduled to discuss the pandemic.
- On March 18, 2020, TWISTED SPIDER announced it will refrain from infecting medical organizations until the pandemic situation stabilizes. Other criminal actors are also reported to be avoiding infections of healthcare sector entities.
- CrowdStrike Intelligence has observed ongoing MUSTANG PANDA activity since late February 2020 using lure content related to the COVID-19 pandemic. Observed incidents have used malicious shortcut files (LNK) to drop decoy documents in Chinese, English and Vietnamese.
- CrowdStrike Intelligence anticipates that hacktivism, particularly in Latin America and Europe, is likely to spike during the global COVID-19 pandemic, judging from hacktivist operations over the past week. During the past year, rates of hacktivism in Latin America have already been higher than normal, due mostly to political unrest in much of the region. These campaigns are likely to increase as other protest options narrow, given that widespread demonstrations and other large gatherings are increasingly prohibited in order to slow the spread of the virus.