Hewlett Packard Enterprise

White Paper

HPE Point of View: COVID-19 Impact on the Cyber Threat Landscape

State and Local Government

Introduction

It is an unfortunate fact that cyber threat actors have wasted no time to leverage the COVID-19 pandemic for their own purposes. In response, security and IT teams in state and local government agencies may have to modify their security policies and priorities, while simultaneously supporting unexpected new service requirements and accommodating changes such as increased remote working. Unfortunately, such agencies may find that they lack the technical infrastructure, staff, and expertise to handle all these challenges at once. As always, information is the starting point for effective security. This POV will detail the changes in cyber threat behavior observed since the outbreak started, as well as highlight relevant HPE security solutions and services.

Exploiting the human element

The threat actors exploiting the COVID-19 situation include both Advanced Persistent Threat (APT) groups (which tend to be well-funded and organized) and cybercriminals. Their primary tactic is to take advantage of human characteristics that are pervasive during the pandemic. Commonly, they try to make themselves appear to be an organization that is trusted; for example, a health organization or government agency. Although the pandemic situation is highly unusual, their goals are consistent with the normal state of affairs: ransomware, data theft, and espionage.[1]

The human characteristics that are being exploited include:

- **Fear:** Perhaps the strongest emotion of all, fear motivates people to take actions they otherwise wouldn't, or to reset their priorities in ways that are difficult to predict.
- **Desire for information:** People crave information about the pandemic and associated topics such as financial stimulus measures. This will lead them to explore digital information sources of dubious or unknown reputation.
- **Distraction:** Employees simply have more pressing concerns as they navigate the pandemic—in particular, the health of their families and having to deal with children out of school. This may make them deprioritize adherence to corporate policies and guidelines for protecting digital assets.

In addition, attackers may leverage gaps in traditional layered defenses that occur as a result of emergency infrastructure changes. For example, if large numbers of people are suddenly expected to work remotely, there may not be time or staff to validate endpoint protections or implement least-privilege network access control policies.

Categories of cyberattacks leveraging today's environment

Several types of attacks that leverage the pandemic have been observed. The most common are:

- **Misinformation:** Well-known social platforms from Facebook on down are inundated with false and misleading information.
- **Fake websites and apps:** A number of information sources purporting to host data of interest are actually repositories for malware, including ransomware.
- **Brand hijacking and abuse:** Threat actors steal known and trusted brands to drive their success. For example, a well-known attacker recently started branding attacks as originating from the Canadian Public Health Agency.
- **Phishing and spear-phishing:** Email-based attacks with COVID-19 content are rampant. Staff in state and local government may be particularly attractive targets for such campaigns because of their access to sensitive data.

As this list makes clear, exploiting human vulnerability is the primary element threat actors are leveraging during the pandemic.

[1] "COVID-19 Exploited by Malicious Cyber Actors." Cybersecurity and Infrastructure Security Agency, April 2020

Suggested risk mitigation actions

Based on the potential impact and likelihood for typical organizations, HPE believes that several actions merit immediate consideration to mitigate the heightened risks during the pandemic:

- **Training:** Just as people need to be educated on how to avoid spreading COVID-19, they need to be re-educated and reminded of email and web policies as well as expectations of employees for avoiding attacks. Organizations should use examples of COVID-19-related attacks already made public to emphasize the seriousness of the threat.
- **E-mail defenses:** Phishing and spear-phishing using COVID-19 content as the lure are rampant. They are designed to deposit Trojans, ransomware, or other malware that delivers a persistent attack payload into the environment. Evaluate whether your solution effectively blocks them, and if your employees are doing their part to alert the IR/SOC team to scams they find in their inbox. Defenses should be tested against actual phishing examples that have surfaced during the pandemic.
- **Malware detection:** In most environments, the biggest risk is that a campaign that leverages the COVID-19 situation will plant malware designed to persist and to execute later stages of the kill chain opportunistically. Detecting such malware is critical given these new insertion strategies based on the virus situation. This is especially true for any organization that works with sensitive data, including state and local government.
- **Brand enforcement:** Government teams should have staff specifically tasked with monitoring the use of their organization's name and reputation on the Internet. Staffing levels and priorities should be reviewed considering the change in the threat landscape. It should be noted that most government IT staff do not have this level of technical staff and may need to consider outsourcing this activity.

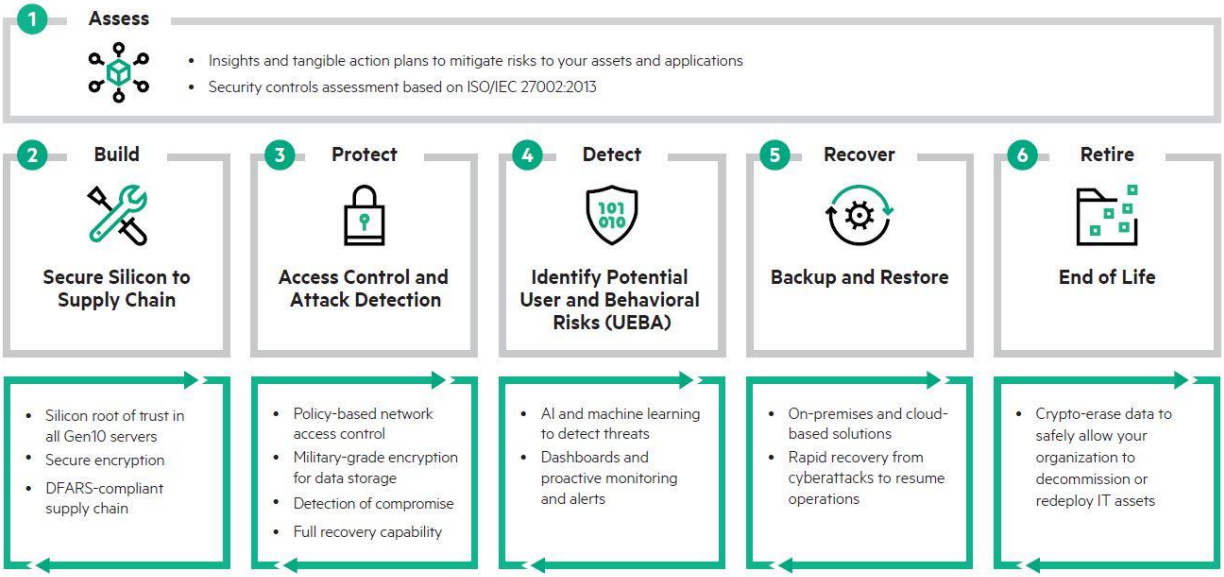
As with all security strategies, a risk-based approach must be applied when making the tough choices and trade-offs associated with cyber security. For example, a government agency may conclude that phishing is the biggest immediate risk and therefore new staff training and email security technical measures are warranted.

HPE cyber security strategy

HPE follows a holistic security strategy to protect your organization's infrastructure for its entire lifecycle. From the hardware supply chain to your device's end of life, HPE provides comprehensive security to detect and prevent unauthorized access as well as rapid recovery from disasters.

HPE uses a six-step model to frame our contributions to an organization's security architecture and infrastructure lifecycle.

AN END-TO-END SECURITY APPROACH



When evaluating the potential risks associated with COVID-19-related threats, three HPE security offerings stand out:

- **Secure server infrastructure:** Gen10 Silicon Root of Trust ensures applications and data reside on a trusted platform.
- **Aruba policy enforcement:** Access infrastructure based on ClearPass and policy enforcement firewalls provides “zero trust” dynamic segmentation and application classification to limit malware propagation. This should be used to segment areas where sensitive data is being generated, processed, or stored, so that malware and advanced persistent threats (APTs) cannot propagate into these areas and exfiltrate such data.
- **HPE Pointnext Services:** Advisory services provide security assessment, recommendation, and remediation services.

Lastly, it should be noted that other HPE solutions gain relevance as building blocks in any architecture that supports application and data availability and accessibility—even in highly stressed environments such as those seen during the COVID-19 pandemic:

- Data Protection and Recovery for Hybrid IT
- Virtual Desktops (VDI)

Summary

The COVID-19 pandemic has provided a fertile environment for innovative new cyberattacks. Threats that leverage the fear and stress people naturally feel at such times can defeat even robust security architectures. HPE recommends education, brand management, and enhanced email and anti-malware defenses as the immediate priorities. IT and Security staff in state and local government should consider both temporary services augmentation and additional technical controls to overcome the short-term demands caused by the pandemic. More broadly, applications and data must reside on resilient infrastructure that drives business continuity but is also highly flexible to support digital transformation.

April 2020