elliott davis

Securing Your Organization

As a result of COVID-19

Introduction

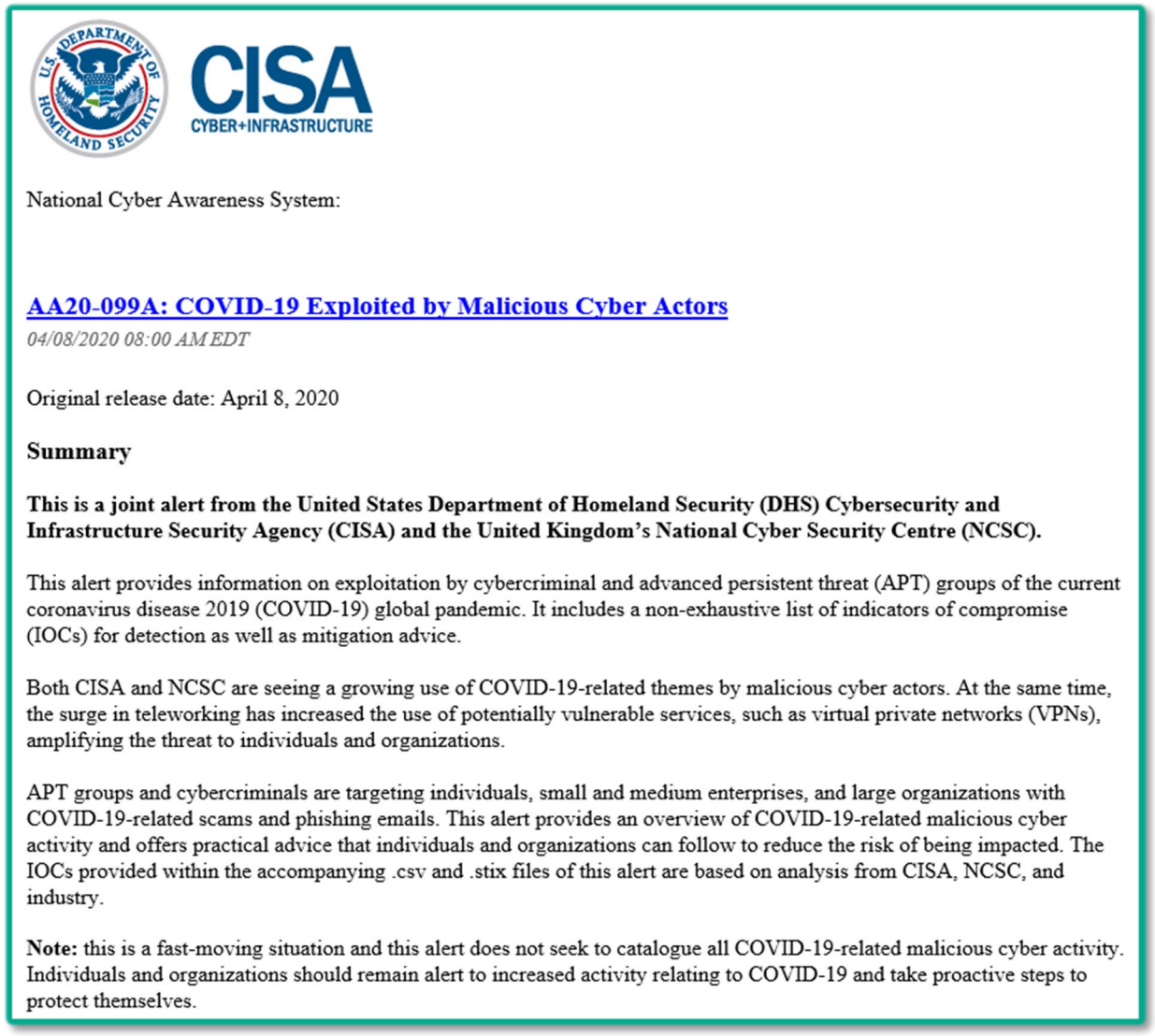
History has proven that cyber criminals increase their attack efforts on organizations when there are other significant events at play such as natural, technological, or manmade disasters. These criminals are now taking advantage of the COVID-19 pandemic with increased attempts to steal data and interrupt business operations through the use of Ransomware.

Many organizations have sent employees home to work remotely to stop the spread of COVID-19. In doing this, the “attack surface” for a cyber criminal to gain access to an organization’s data and critical systems has expanded. This expanded attack surface along with the increase in threats, is creating the perfect storm for an organization to fall victim to an attack.

In this document, the Elliott Davis Risk Advisory and Cybersecurity Team recommends certain steps be performed **as soon as possible** to mitigate this increased risk.

We stand ready to assist you!

Jimmy Buddenberg
Director of Risk Advisory & Cybersecurity Services



CISA
CYBER+INFRASTRUCTURE

National Cyber Awareness System:

AA20-099A: COVID-19 Exploited by Malicious Cyber Actors

04/08/2020 08:00 AM EDT

Original release date: April 8, 2020

Summary

This is a joint alert from the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom’s National Cyber Security Centre (NCSC).

This alert provides information on exploitation by cybercriminal and advanced persistent threat (APT) groups of the current coronavirus disease 2019 (COVID-19) global pandemic. It includes a non-exhaustive list of indicators of compromise (IOCs) for detection as well as mitigation advice.

Both CISA and NCSC are seeing a growing use of COVID-19-related themes by malicious cyber actors. At the same time, the surge in teleworking has increased the use of potentially vulnerable services, such as virtual private networks (VPNs), amplifying the threat to individuals and organizations.

APT groups and cybercriminals are targeting individuals, small and medium enterprises, and large organizations with COVID-19-related scams and phishing emails. This alert provides an overview of COVID-19-related malicious cyber activity and offers practical advice that individuals and organizations can follow to reduce the risk of being impacted. The IOCs provided within the accompanying .csv and .stix files of this alert are based on analysis from CISA, NCSC, and industry.

Note: this is a fast-moving situation and this alert does not seek to catalogue all COVID-19-related malicious cyber activity. Individuals and organizations should remain alert to increased activity relating to COVID-19 and take proactive steps to protect themselves.

US Department of Homeland Security Cyber Bulletin

elliott davis

Recommended Actions to Take

Action #1: Review Remote Access Policy and Provide Recommendations
With the lines between home and corporate networks being blurred, organizations should clarify acceptable and unacceptable uses of technology to reduce the risk of employees inadvertently introducing cybersecurity threats to the environment.

Action #2: Provide Cyber Awareness Training to Employees - Including Proper and Secure Data Storage
Awareness training plans need to be updated to reflect employees staying and working from home almost exclusively during the pandemic. Users should also be educated on proper areas for file storage and transfer while out of the office.

Action #3: Evaluate Whether There are Unsecured Remote Access Products (e.g. RDP) Exposed to the Internet
Unsecure instances of Remote Desktop Protocol (RDP) are one of the leading contributors of Ransomware attacks against organizations. With new remote access solutions being configured and rolled out in a short amount of time, organizations should test them for weaknesses that can be exploited by criminals.

Action #4: Review VPN Authentication Methods and Assist in the Setup of Multi-factor Authentication if Needed
Organizations should have a third party review their VPN connectivity to verify proper security controls are in place as attackers are working to leverage newly implemented VPN's for their attacks. Multi-factor authentication should be enabled for all remote users to protect the organization from compromise.

Action #5: Review Antivirus and Patch Management Procedures
With a remote workforce now in place, previous controls regarding patching of systems and updating antivirus may no longer be working properly. A review of key patching and virus technologies is necessary to make sure they are functioning properly across remote connections.

Recommended Actions to Take

Action #6: Perform a Review of Network Administrative Groups
Many organizations have rushed to implement new technologies to support a remote work force and it is possible that additional permissions were temporarily given to users and support personnel to facilitate the changes. Now is the time to review these groups to make sure they are secured.

Action #7: Check the Integrity of Backups and Failover Systems
With an increased attack surface, it is more important than ever for organizations to verify that they can restore their organization quickly in the event of a significant outage or cyberattack. The speed in which an organization can recover its systems should be communicated and agreed to by senior management.

Action #8: Examine Network for Abnormally Long Connections That Could Be Indicative of a Cyber Attack
Persistent connections to external entities can represent attackers communicating to command and control centers or tunneling information out of the network. Reviewing network logs and firewalls for these types of connections is a best practice.

Action #9: Review Other Changes Made to Enable Remote Access and Secure According to Best Practices
An audit of existing remote access policies (split tunneling for example) is necessary to make sure that newly implemented remote connectivity does not reduce the security posture of the organization.

Recommended Actions to Take

Action #10: Perform a Full External Network Scan to Determine all Exposed Ports

Now that all new remote access technologies are in place, organizations should have a third party perform an external vulnerability scan to verify that only the ports and protocols necessary for remote access are enabled. We often see organizations misconfigure firewall rules, which increases an organization's attack surface.

Action #11: Review and Assist in Configuring Firewall Rules to Best Practices

A review of firewall rules (especially those implemented quickly for remote access) is a good idea to ensure an organization is following best practice in regards to the security of its perimeter.

Action #12: Perform a Full Cyber Security Assessment (scorecard) and Issue a Formal Report

Cyber assessments against an industry framework assist organizations with understanding their key areas of risk and how they should invest in future initiatives to reduce overall risk.

Action #13: Perform a Full Network Penetration Test and Issue a Formal Report

A network penetration test will simulate the actions of an attacker and provide an organization with key areas that need improvement to keep attackers off their network. When evaluating customer environments, it is important to evaluate all technologies including any web applications developed internally or by third parties. Web applications often leak key information on employees and products and can also provide a conduit for an attack on a company's infrastructure.

Action #12: Cybersecurity Assessment Scorecard

		CIS Control	Policy	Implementation	Reporting	Weighted Average	Grade
Basic	1	Inventory and Control of Hardware Assets	60%	77%	70%	75%	C
	2	Inventory and Control of Software Assets	56%	71%	72%	70%	C-
	3	Continuous Vulnerability Management	48%	59%	57%	58%	F
	4	Controlled Use of Administrative Privileges	79%	81%	85%	81%	B-
	5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	70%	87%	87%	85%	B
	6	Maintenance, Monitoring and Analysis of Audit Logs	63%	86%	83%	83%	B
		Basic Controls - Results	**63%**	**77%**	**76%**	**75%**	**C**
Foundation	7	Email and Web Browser Protections	46%	60%	58%	58%	F
	8	Malware Defenses	53%	72%	72%	70%	C-
	9	Limitation and Control of Network Ports, Protocols, and Services	70%	87%	87%	85%	B
	10	Data Recovery Capabilities	100%	100%	93%	99%	A+
	11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	70%	93%	89%	90%	A-
	12	Boundary Defense	66%	80%	80%	79%	C+
	13	Data Protection	57%	52%	52%	53%	F
	14	Controlled Access Based on the Need to Know	63%	79%	79%	77%	C+
	15	Wireless Access Control	53%	69%	69%	67%	D+
	16	Account Monitoring and Control	67%	85%	84%	83%	B
		Foundational Controls - Results	**65%**	**78%**	**76%**	**76%**	**C**
Organization	17	Implement a Security Awareness and Training Program	42%	66%	28%	60%	D-
	18	Application Software Security	67%	80%	79%	79%	C+
	19	Incident Response and Management	86%	77%	77%	78%	C+
	20	Penetration Tests and Red Team Exercises	28%	28%	28%	28%	F
		Organizational Controls - Results	**56%**	**63%**	**53%**	**61%**	**D-**
		Overall Grade	**63%**	**75%**	**73%**	**74%**	**C**

As an output of our cybersecurity assessment, you will receive an overall ‘scorecard’ (example above), a detailed assessment report including scope of the assessment, log of assessment findings, remediation recommendations, and a summary overview for management.

Scope of Value

Services	Ultimate	Premium	Essential
1. Review remote access policy and provide recommendations	✓	✓	✓
2. Provide cyber awareness training to employees including proper and secure data storage	✓	✓	✓
3. Evaluate whether there are unsecured remote access products (e.g. RDP) exposed to the Internet	✓	✓	✓
4. Review VPN authentication methods and assist in the setup of multi-factor authentication if needed	✓	✓	✓
5. Review antivirus and patch management procedures	✓	✓	✓
6. Perform a review of network administrative groups	✓	✓	✓
7. Check the integrity of backups and failover systems	✓	✓	✓
8. Examine network for abnormally long connections that could be indicative of a cyber attack	✓	✓	✓
9. Review other changes made to enable remote access and secure according to best practices	✓	✓	✓
10. Perform a full external network scan to determine all exposed ports	✓	✓	
11. Review and assist in configuring firewall rules to best practices	✓	✓	
12. Perform a full cyber security assessment (scorecard) and issue a formal report	✓	✓	
13. Perform a full network penetration test and issue a formal report	✓		
Payment Terms	25% Prepayment	50% Prepayment	75% Prepayment
Price	**$ TBD**	**$ TBD**	**$ TBD**

Please reach out with questions

Jimmy.Buddenberg@elliottdavis.com

864.250.3936

elliott davis