KROLL

Cybersecurity

Looking Back, Looking Forward

June 6, 2022

Kroll – Protecting People and Property

Why Are We Talking About This?

- There is a hacker attack every 39 seconds
- 43% of cyber attacks target small business
- 85% of successful breaches target humans
- The average cost of a data breach in 2020 will exceed $4 million
- In 2020 estimates say 36 billion personal records were exposed from breaches (up from 7.9 billion in 2019)
- 65% of security professionals surveyed expect to be responding to a major breach in the next year

Top Cybersecurity Topics

Ransomware	**Phishing**	**Internet of Things (IoT)**
Business Email Compromise (BEC)	**COVID-19 Attacks**	**Regulatory Changes**

Impacts

Financial

- Business interruption, theft of funds, destruction of equipment
- Raises in cyber insurance premiums
- Lawsuits

Reputational

- Loss of confidence in your Company, your product, your brand

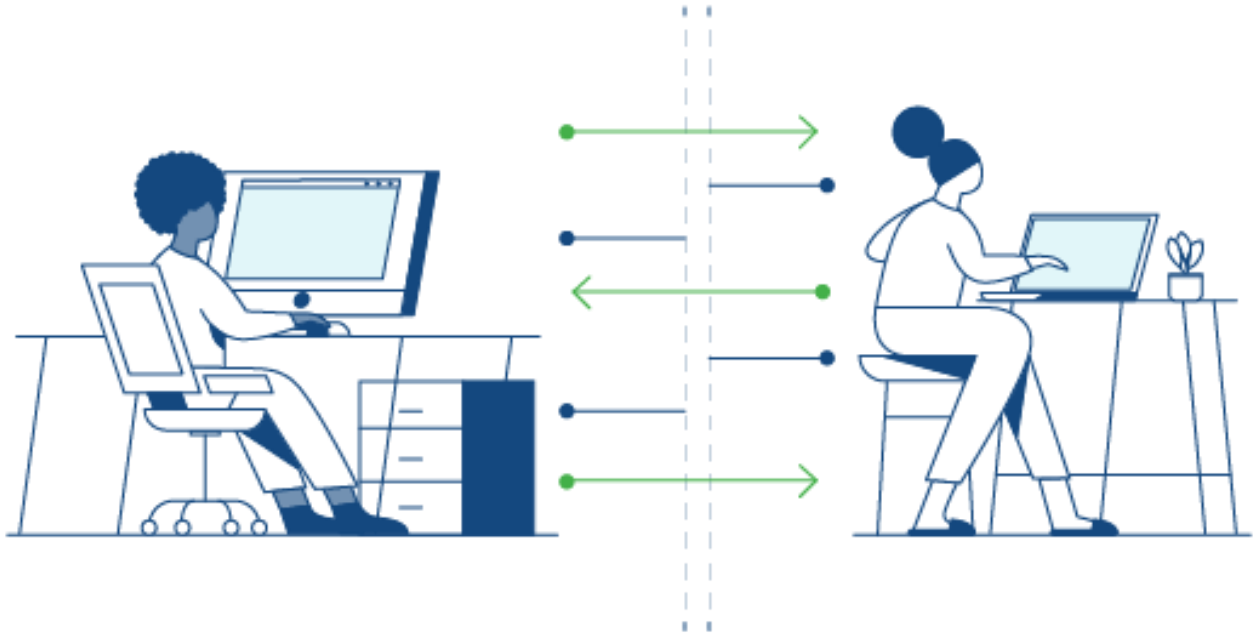
Governmental Impacts

- Loss of infrastructure use, loss of confidence in government
- Potential for impact to hardware (ties into IOT)
- Targeting by Hostile Intelligence Services

Best Practices – Business

Preparedness and Hygiene

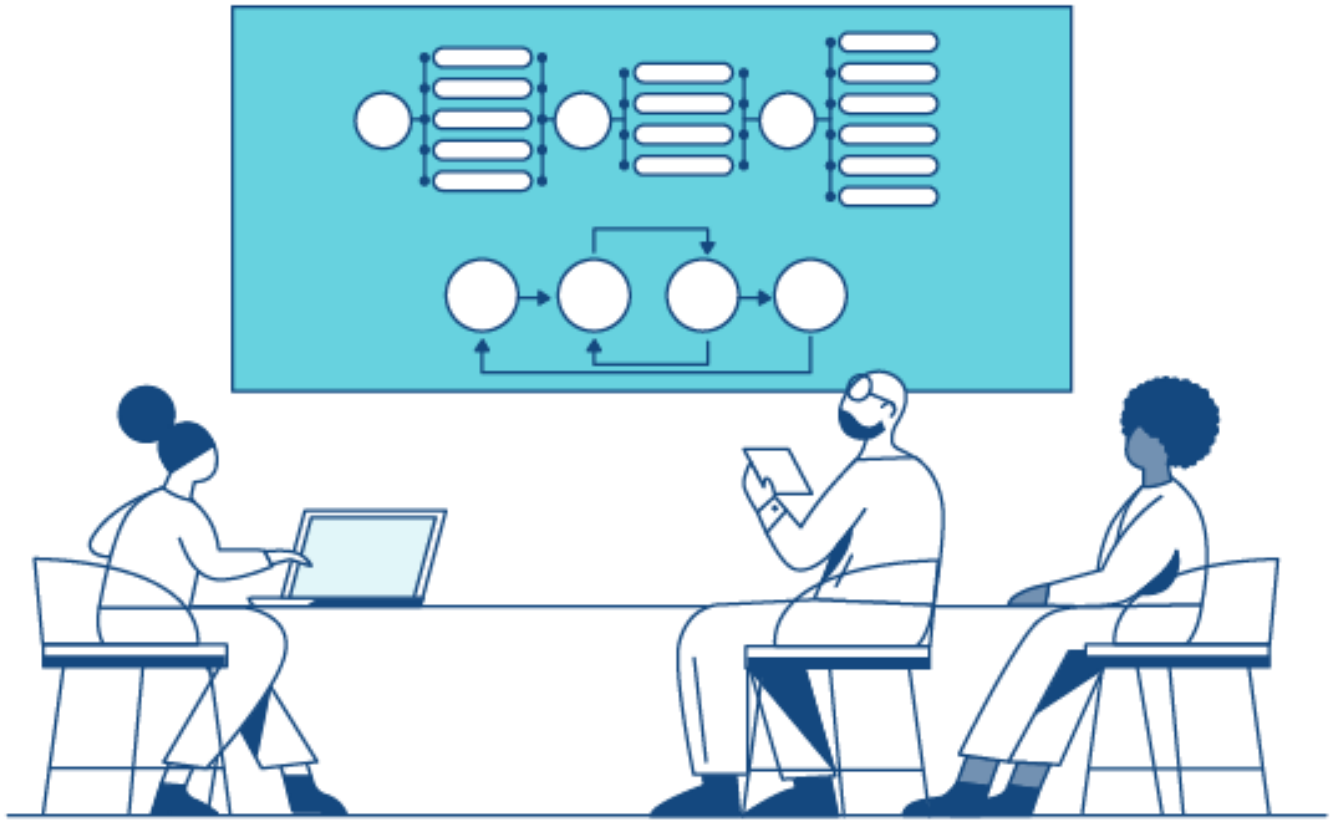
- Regular offsite backups
- Vulnerability assessments
- Reduce the surface area for the attack
- Segmentation



Best Practices – Business

Cyber Resiliency

- Have an incident plan
- Ensure everyone knows the plan
- Train to the plan
- Learn and modify



Resiliency Key Components

- Anticipate the threats
- Preparation
- Response
- Remediation/Recovery

From: Kroll Responder Team
Sent: Wednesday, September 9, 2020 9:51 AM
Subject: Kroll Response- [ALERT-14] Malicious Software (Ransomware) affecting l-12345.contoso.com

Threat Detection	ALERT-14
Status	Acknowledged > **Contained** > Remediated
Action Required to Remediate	• Reset password of user accounts: **Administrator** and **A013215**.
Hostname (IP Address)	l-12345.contoso.com (10.13.25.6)
Username	CONTOSO\A013215
Incident Summary	At 2020-09-09 08:21:09 UTC, Kroll observed the execution of a malicious binary *"c:\users\a013215\desktop\svchost\svchost.exe"* which was masquerading as the Windows Service Host (svchost.exe). Kroll found this binary to be associated with **Spade Ransomware** which encrypts and renames files using a *".spade"* file extension. Upon further investigation, Kroll found that the threat actor leveraged an open Remote Desktop Protocol (RDP) [TCP/3389] connection to the laptop, and authenticated to the system using the account **A013215**, originating from source IP ***92.xx.xx[.]xx***. The ransomware binary also made a connection to IP *94.xx.xx[.]xx*. Events related to open RDP were observed for the same host in the detection ALERT-13.
Kroll Response Actions	• Terminated the active RDP session. • Terminated all associated running processes. • Banned the hash of the malicious file. • Isolated the laptop to stop further spread of Ransomware into the network.

Recommendations	• Block the following IPs on perimeter devices:
	  ○ *92.xx.xx[.]xx*
	  ○ *94.xx.xx[.]xx*
	• Review RDP authentication and access policies.
	• Contact your Kroll team with any questions on the above recommendations.

Best Practices – Personal

Personal Networks/Devices

- Update your devices often and automatically
- Change default username/passwords/network names
  - Home security systems, routers, etc.
- Leverage security software and keep it current
- Encrypt your device and media

KROLL

For more information, please contact:

Timothy Gallagher
Managing Director
Cyber Risk
New York
+1 646 899 6973
timothy.gallagher@kroll.com

Patrick Grobbel
Managing Director
Data Insights and Forensics
Washington, D.C.
+1 202 256 7608
patrick.grobbel@kroll.com

About Kroll

Kroll provides proprietary data, technology and insights to help our clients stay ahead of complex demands related to risk, governance and growth. Our solutions deliver a powerful competitive advantage, enabling faster, smarter and more sustainable decisions. With 5,000 experts around the world, we create value and impact for our clients and communities. To learn more, visit www.kroll.com.