Secureworks®

Mid-Atlantic CIO Forum

Ryan Alban, CISSP | GISP
Sr. Manager,
Global Solution Leads,
Extended Detection & Response

Timeline slide intentionally removed for distribution.

- This is what a divider slide looks like.

Secureworks®

Today's Topics

- A Tale of Two Threat Actors: A SolarWinds Retrospective
  - SUNBURST
  - SUPERNOVA
- You Get A Webshell!
- The CIA & Cyber-Crime
- What can we learn?

SUNBURST

- This is what a divider slide looks like.

Timeline slide intentionally removed for distribution.

- This is what a divider slide looks like.

A Skilled & Patient Adversary

Excellent Operational Security

Low Profile

- 2-week dormancy period before beaconing
- US-hosted infrastructure
- Novel compile-time code injection technique
- Signed binary deployed

Selective Targeting

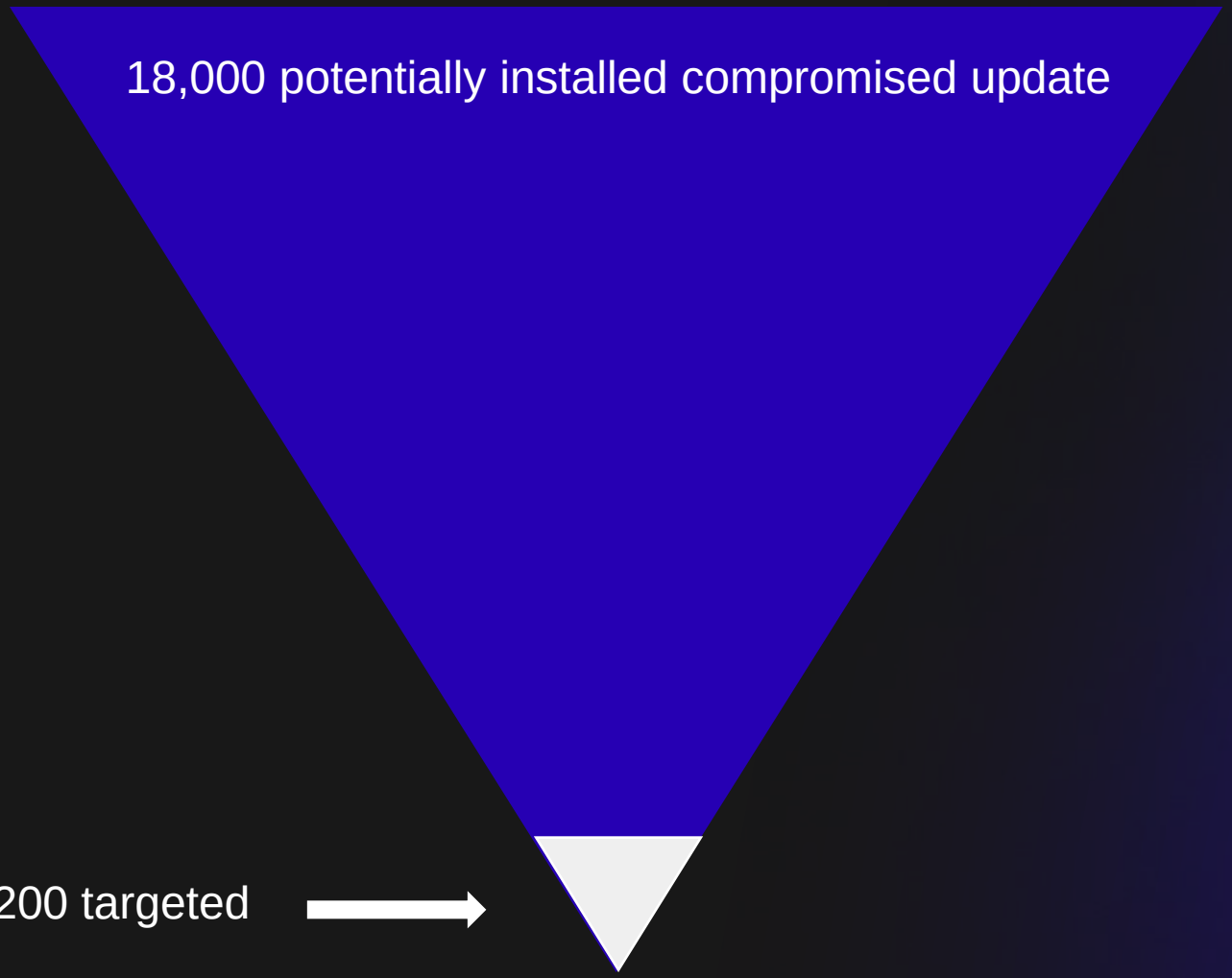
- Remediated non-targeted intrusions

Bespoke IoCs

- Cobalt Strike DLL implants
- Folder names
- File names
- C2 domains
- IPs, HTTP requests,
- Etc.

Incident Response Questions

Capability + Opportunity + Intent



Secureworks®

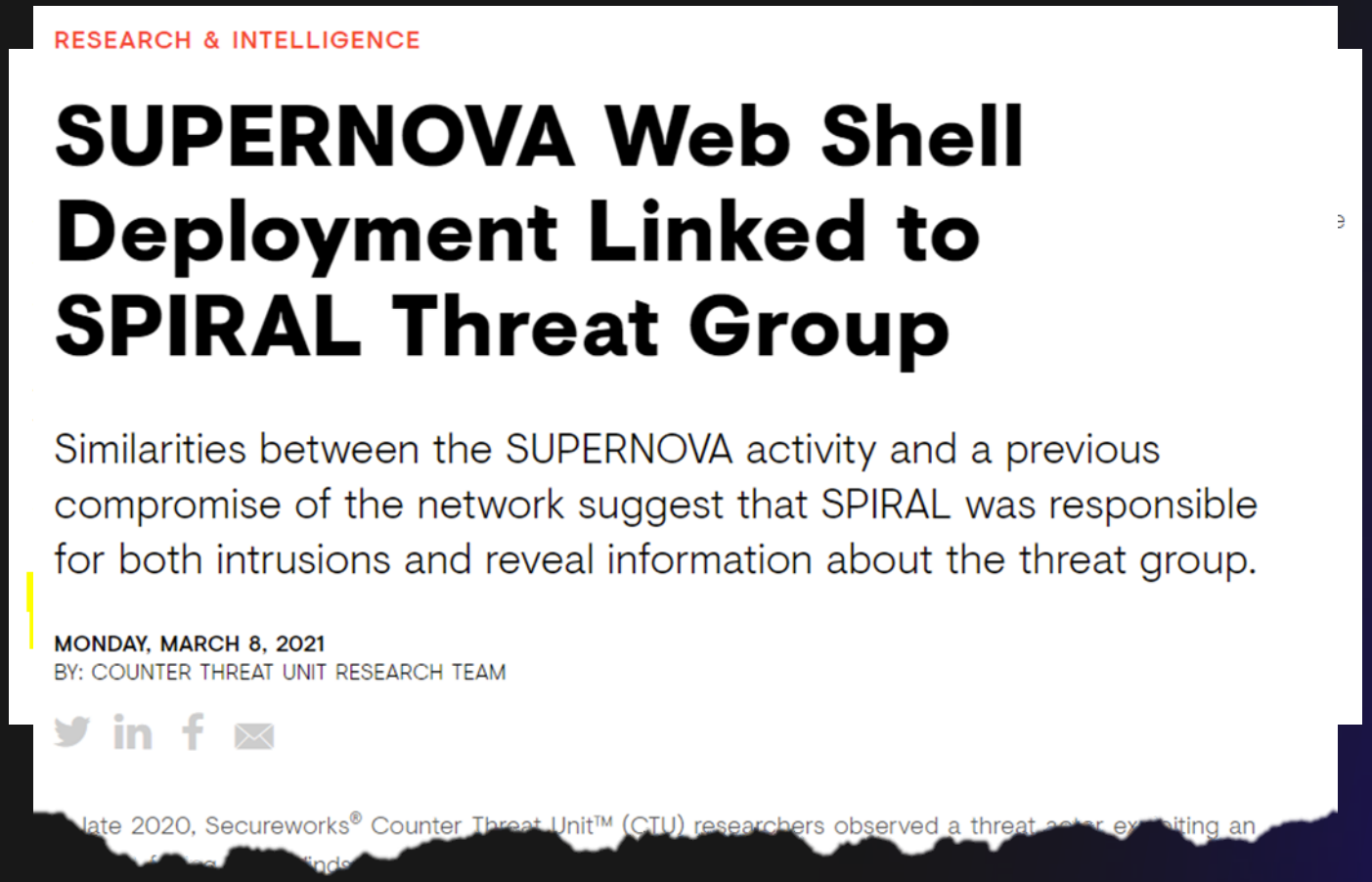
SUPERNOVA

- This is what a divider slide looks like.

Timeline slide intentionally removed for distribution.

- This is what a divider slide looks like.

The Rest of the Story



RESEARCH & INTELLIGENCE

SUPERNOVA Web Shell Deployment Linked to SPIRAL Threat Group

Similarities between the SUPERNOVA activity and a previous compromise of the network suggest that SPIRAL was responsible for both intrusions and reveal information about the threat group.

MONDAY, MARCH 8, 2021
BY: COUNTER THREAT UNIT RESEARCH TEAM

late 2020, Secureworks® Counter Threat Unit™ (CTU) researchers observed a threat actor exploiting an

Standard APT

Unremarkable TTPs

Vulnerability Exploit

- Authentication bypass flaw
- Installed a modified SolarWinds binary (webshell)
- Modified binary was improperly signed by attacker

Webshell

- Fairly standard webshell capabilities
- Credential Dumping and Exfil

Lateral Movement

- Map drive to Domain Controller
- Access to business-sensitive data

Related but Different

One Software, 2 different campaigns

	SUNBURST	SUPERNOVA
Software at Issue	SolarWinds Orion Platform	SolarWinds Orion Platform
Distribution	SolarWinds Software Update	Exploit Vulnerability of API (externally-facing systems)
Attack Methods	Quiet and Surgical Strong Operational Security	Typical APT
Adversary	Likely Russian Intelligence	Likely Chinese

Managing Supply Chain Risk

Ask yourself….

- How is this product or service used in my environment?
- What data does it have access to?
- What credentials does it have access to?
  - Are these credentials privileged?
  - Do these credentials have broad access to other resources?
- How accessible is this product or service in my environment?
  - Does it access the Internet?
  - Does the Internet have access to it?
- What logging and visibility do I have to this product or service?

A Case of the Mondays

“Hello CTU, we have been seeing multiple clients being targeted by a similar attack.”

Secureworks®

Microsoft Exchange Server RCE

RESEARCH & INTELLIGENCE

Government-Sponsored

This combination of exploitation technique and use of China Chopper made this activity particularly puzzling. Exploits for vulnerabilities that do not have a patch (also known as 'zero-days') are rare. Most government-sponsored actors avoid using zero-days because they don't need to. Zero-days affecting Exchange are even rarer and are incredibly valuable because unauthenticated remote code execution on mail servers is a very bad thing. It was therefore surprising that the threat actors 'burned' valuable exploits by executing malware that would be quickly detected by many security vendors.

So why do it?

THURSDAY, MARCH 4, 2021
BY: MIKE MCLELLAN - SECUREWORKS DIRECTOR OF INTELLIGENCE

Managing ~~Supply Chain~~ Software Vulnerability Risk

Ask yourself….

- How is this product or service used in my environment?
- What data does it have access to?
- What credentials does it have access to?
  - Are these credentials privileged?
  - Do these credentials have broad access to other resources?
- How accessible is this product or service in my environment?
  - Does it access the Internet?
  - Does the Internet have access to it?
- What logging and visibility do I have to this product or service?

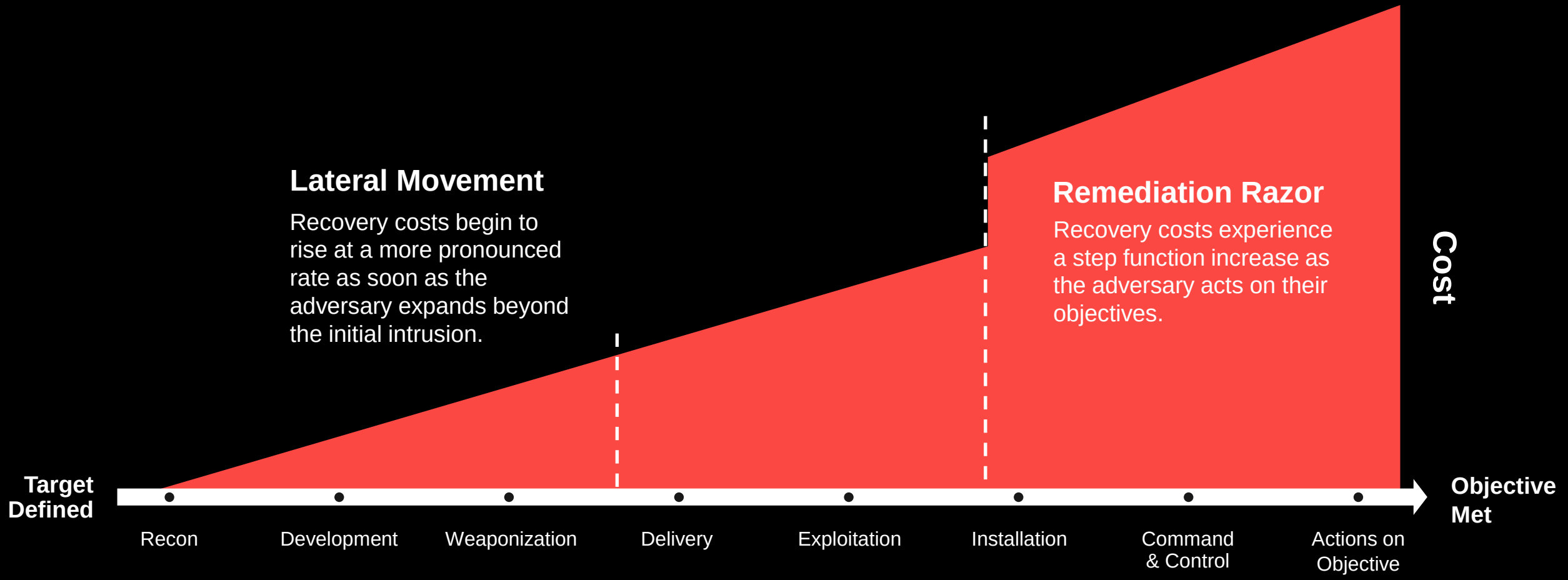
“(Post-Intrusion) Ransomware is still the number one threat our clients face.”

Similar Tactics, Different Objectives & Outcomes

Defending Nation-State Intrusions is difficult (impossible?)…
but not defending against Criminal Intrusions is painful (existential?)…

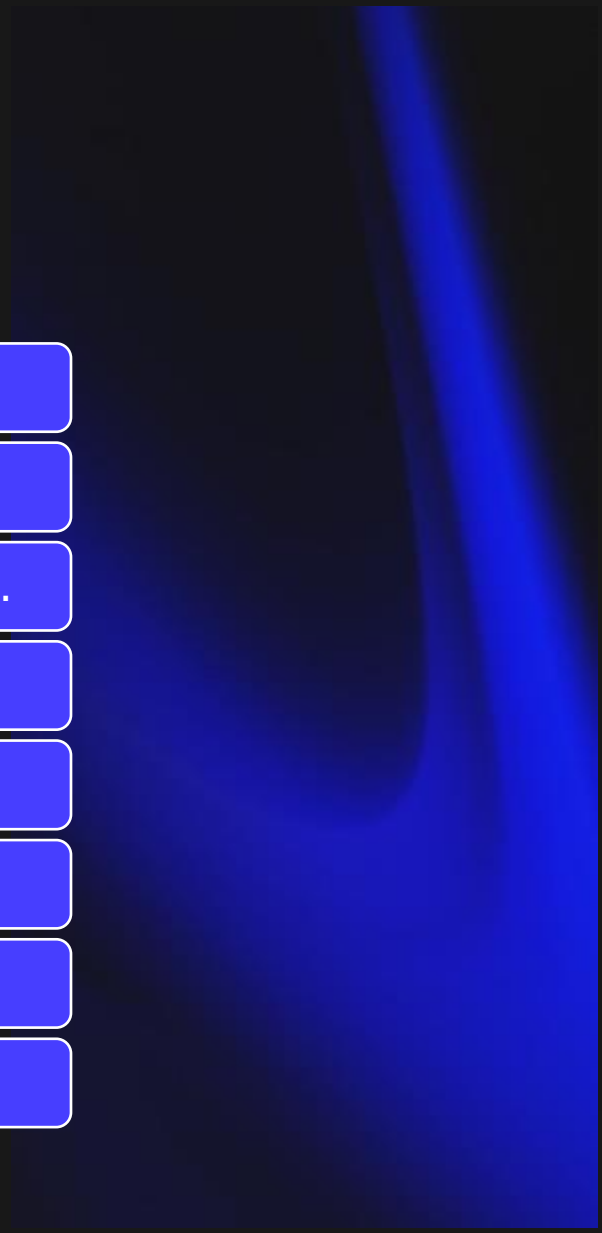
	Nation-State / Espionage	Organized Crime / Financial Gain
C	Makes unauthorized copies of sensitive data. Transfers those copies from the victim network as the primary objective.	Makes unauthorized copies of sensitive data. Transfers those copies from the victim network as the secondary objective.
I	Rarely tampers with integrity of files. Mission is to maintain long-term persistent access and continue to siphon copies of sensitive data from the environment.	Encrypts files so they become unusable. This is primary objective to extort money from victim. Destroys backups to make recovery impossible.
A	Rarely threatens availability. Mission is to maintain long-term persistent access. Disrupting availability disrupts ability to collect.	Act of encrypting files will harm enterprise availability.

The Mission Is Simple: Time to Detect & Respond is Key



What can we learn from these events?

- “Log Retention” can be useful for more than satisfying compliance requirements.
- 30 days is no longer enough for EDR telemetry retention.
- Defending against nation states is hard, not defending against criminals is painful.
- Nation-State capabilities eventually trickle down to Cyber-Criminals.
- Even Nation-State actors make mistakes.
- Deploy software updates immediately(!?!)
- Cloud Services are not perfect but are likely better than the alternative.
- The only differences between “software” and “malware” is *intent.*



Secureworks®

Resources and References

- SolarWinds and the Next Steps for Cybersecurity | Secureworks
- SUPERNOVA Web Shell Deployment Linked to SPIRAL Threat Group Blog | Secureworks
- Government-Sponsored Campaign Targets Microsoft Exchange Vulnerabilities Blog | Secureworks
- Hello CTU, we have been seeing multiple clients being targeted by a similar attack. | Secureworks
- One-Click Microsoft Exchange On-Premises Mitigation Tool – March 2021 – Microsoft Security Response Center
- Ransomware is the Number One Cyber Threat to Organizations Today | Secureworks

thank you.

Secureworks®