Digital Security – Expanding Your Technical Awareness

John Giordano
Cybersecurity Account Executive,
SecureWorks

Neal McCarthy
Cyber Security Incident Response
Consultant
SecureWorks

Sean McLean, PMP
IT Director
Petrinovich Pugh & Company LLP

SecureWorks

Partnering to Fight Cybercrime

Cybersecurity Threat Insights Report for Leaders

SecureWorks

Cybersecurity Analysis Overview

- Analysis of 163 client engagements over the course of the first half of 2016

163
CLIENT ENGAGEMENTS

- Captured and analyzed by:

Global Counter Threat Operations Centers monitoring more than 4,300 organizations' networks 24x7.

Our incident response teams reacting to security incidents every day.

More than 80 Counter Threat Unit™ (CTU) Researchers monitoring and evaluating the latest threat trends.

How are Organizations Faring in Countering Cyber Threats?

Organizations Struggle with the Basics

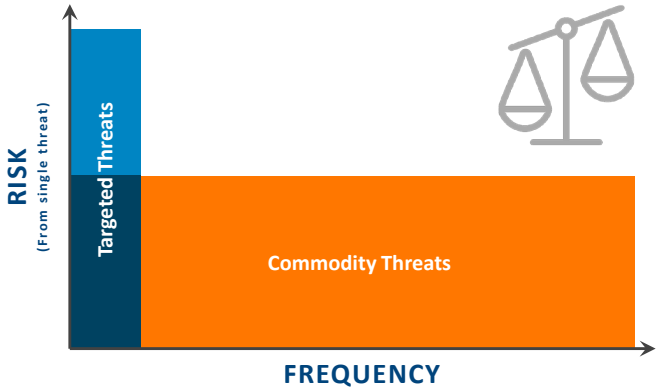
- The industry has lost focus, pushing new technology before adopting security fundamentals

OVER 40%

COMPLIANCE VS SECURITY

- Compliance-Driven security is not the answer. As much as 40% of security staff time is spent on compliance initiatives rather than security initiatives at some financial institutions.

- Striking a balance on risk:
  Targeted threats vs. commodity threats



Organizations are placing undue emphasis and resources on combating advanced threats when commodity threats present a greater likelihood of attack and associated risk.

Organizations Can Do More to Protect Themselves

- Understand the Extended Enterprise
- Increase Visibility
- Build a Culture of Security
- Train Your Users – #1 Risk is Your Employees
- Be Prepared to Respond to Incidents

Perception vs Reality…whats the real problem?

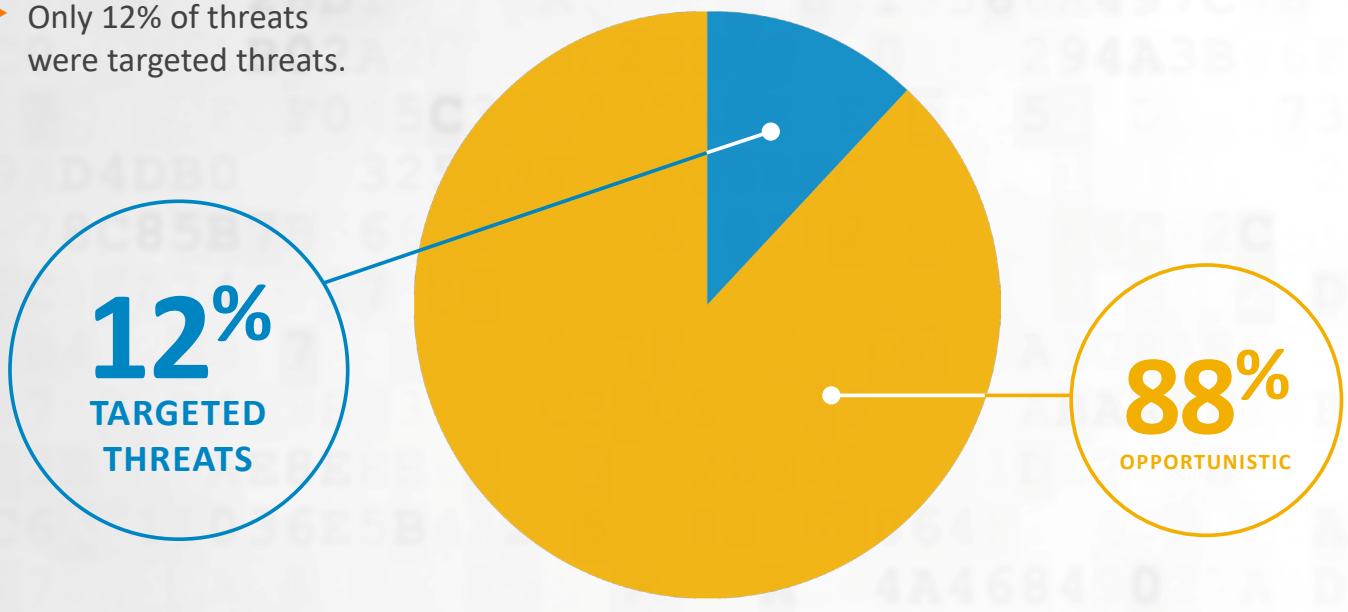
SecureWorks

Financially Motivated Criminality is one of the Main Catalysts of Cyber Incidents

- Here's what we're seeing
  - Financial theft from bank accounts
  - Financial information theft
  - Personal data theft
  - Holding to ransom
  - Theft of computing power (Botnets)

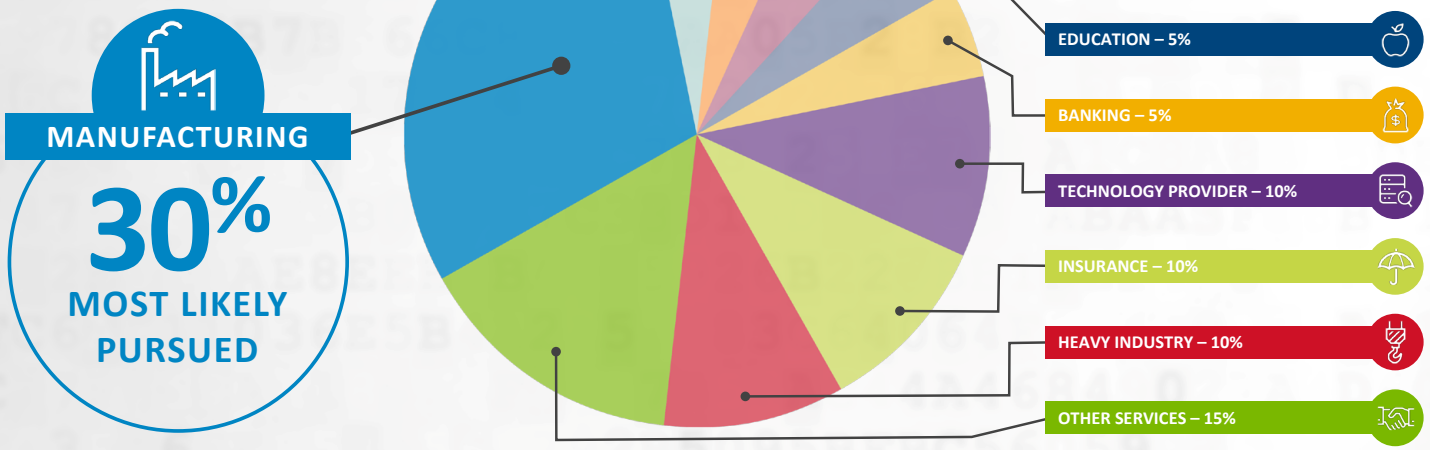
Type of Threat | 2016 Q1/Q2

- Only 12% of threats were targeted threats.



Targeted IR by Industry Vertical | 2016 Q1/Q2

> What Industry is most likely to be pursued by a Targeted Threat – Manufacturing at 30%



How do the bad guys continue to succeed?

SecureWorks

Primary Tactics Used by Hackers

Compromise of vulnerable public-facing systems

Malware is delivered in an email

Third-Party Compromise

Legitimate credentials are compromised

Malware is downloaded from a website

Initial Access Vector | 2016 Q1/Q2

> Initial Access Vector Adversaries leveraged to Initially Gain Foothold in a Victims Environment

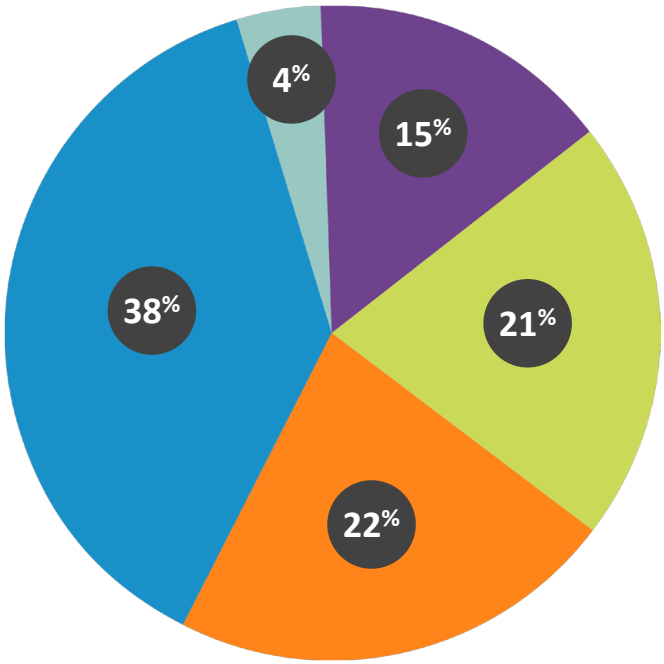
PHISHING

SCAN & EXPLOIT

SWC

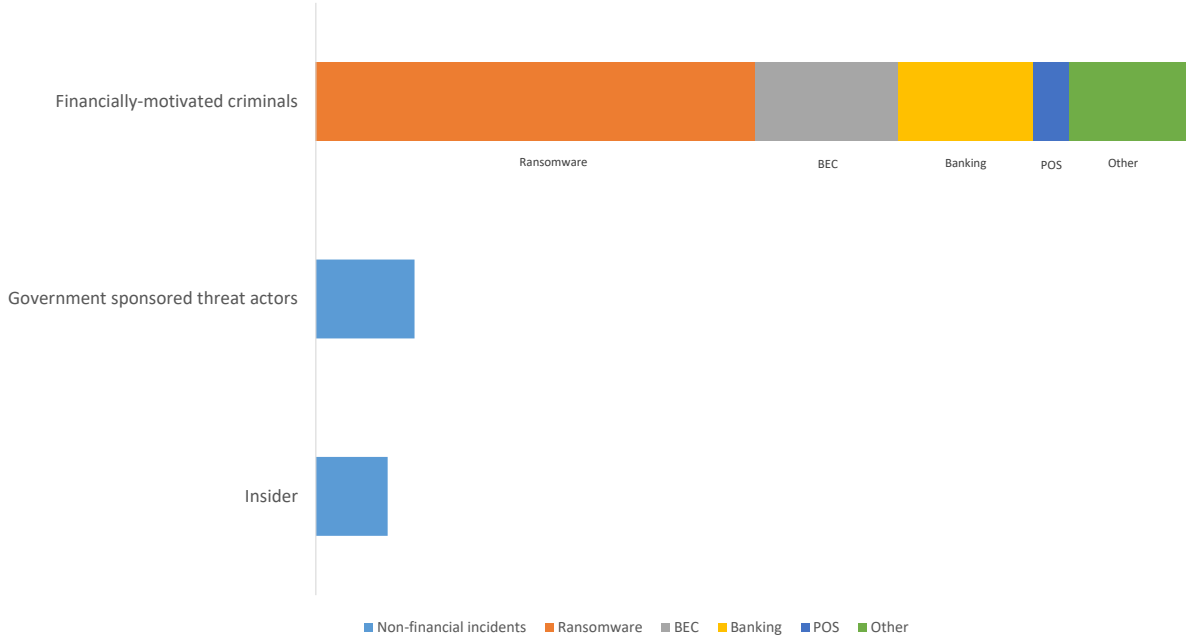
CREDENTIALS

REMOVABLE MEDIA

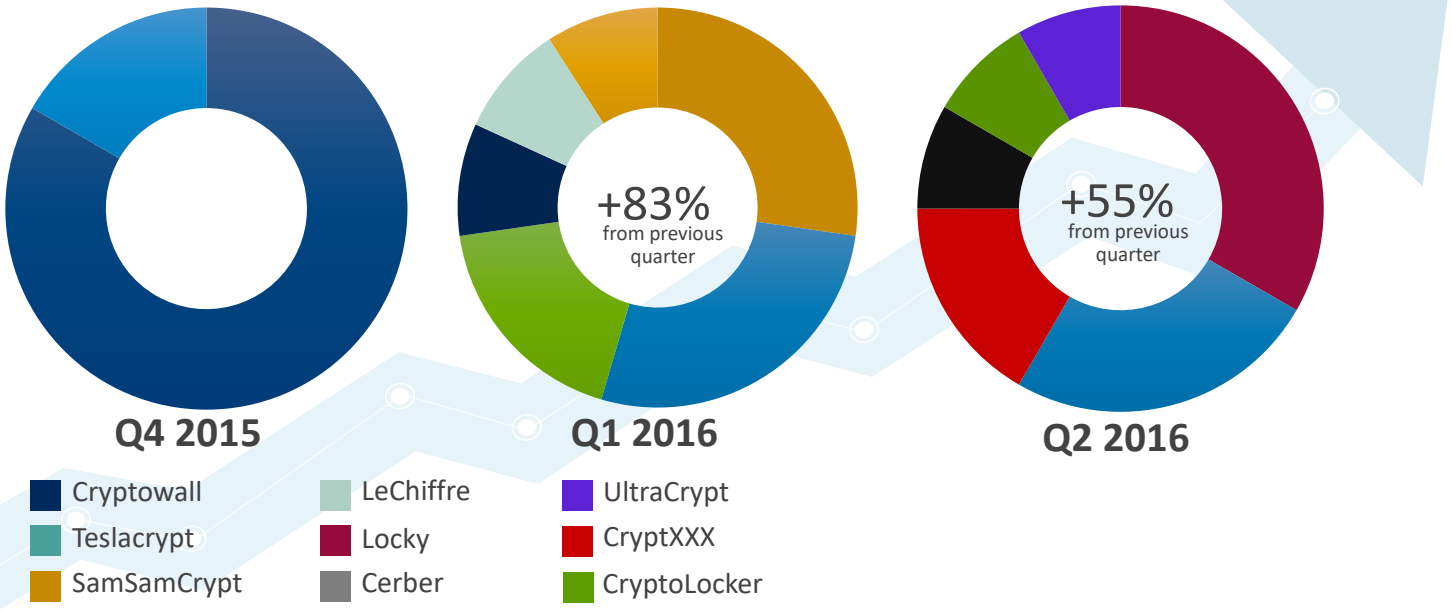


Note: 16% of engagements did not have sufficient information and logging to establish how the adversary got in. This was removed from the data set shown above.

2016 Incidents



Ransomware Incidents

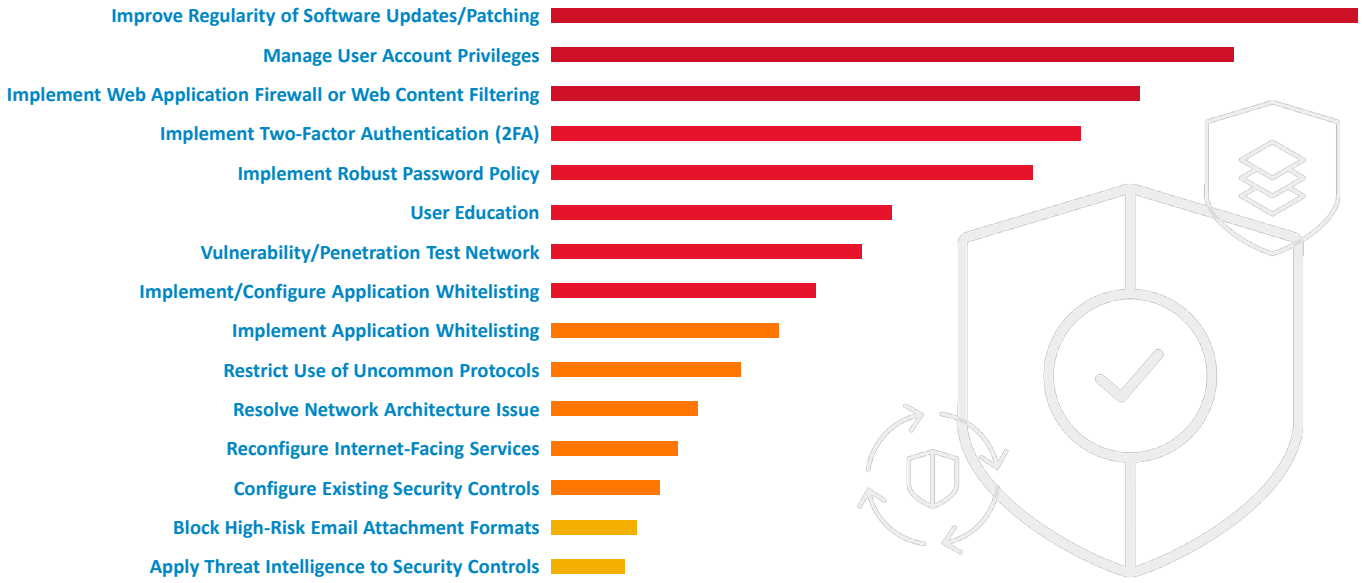


What steps can be taken to minimize the impact?

SecureWorks

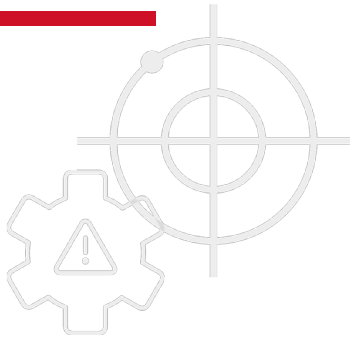
Recommendations for Improving Security

PREVENTION | 2016 Q1/Q2



Recommendations for Improving Security

DETECTION | 2016 Q1/Q2



RESPONSE | 2016 Q1/Q2

Summary

- Threat actors are using the same tried and true methods because they continue to work
- Recalibrate the emphasis on security technologies and prioritize developing strong security postures
- Master the Basics and focus on security fundamentals first
- Look for a strategic security partner who can serve as a trusted advisor