Cautionary Statement Regarding Forward-Looking Statements

This presentation includes express and implied “forward-looking statements”, including forward-looking statement within the meaning of the Private Securities Litigation Reform Act of 1995. Forward-looking statements include all statements that are not historical facts, and in some cases, can be identified by terms such as “anticipate,” “believe,” “estimate,” “expect,” “intend,” “may,” “might,” “plan,” “project,” “will,” “would,” “should,” “could,” “can,” “predict,” “potential,” “continue,” or the negative of these terms, and similar expressions that concern our expectations, strategy, plans or intentions. Forward-looking statements contained in this presentation include, but are not limited to, statements concerning the performance and benefits of our platform, products and services; our strategic plans or objectives; our growth prospects; and our future financial and operational performance. By their nature, these statements are subject to numerous risks and uncertainties, including factors beyond our control, that could cause actual results, performance or achievement to differ materially and adversely from those anticipated or implied in the statements. These and other risk factors are described in the “Risk Factors” section of our most recent Form 10-Q and/or Form 10-K filed with the Securities and Exchange Commission. You should not rely upon forward-looking statements as predictions of future events. Although our management believes that the expectations reflected in our statements are reasonable, we cannot guarantee that the future results, levels of activity, performance or events and circumstances described in the forward-looking statements will be achieved or occur. Recipients are cautioned not to place undue reliance on these forward-looking statements, which speak only as of the date such statements are made and should not be construed as statements of fact. Except to the extent required by federal securities laws, we undertake no obligation to update these forward-looking statements to reflect events or circumstances after the date hereof, or to reflect the occurrence of unanticipated events.
A Dharma Initiative: How OverWatch Threat Hunting Uncovered a Widespread Ransomware Network

Karl Scheuerman, Senior Strategic Intrusion Analyst, CrowdStrike
Aaron Pickett, Senior Strategic Intrusion Analyst, CrowdStrike
Agenda

- Current eCrime Trends
- Dharma Ransomware
- Threat Hunting for Dharma
- Conclusions & Recommendations
Karl Scheuerman
Senior Strategic Intrusion Analyst

- 10+ years of experience in intelligence and security
- Air Force/Air National Guard
- OverWatch threat hunter
- Twitter: @KarlScheuerman
- Email: karl.scheuerman@crowdstrike.com
Aaron Pickett
Senior Strategic Intrusion Analyst

- Security and intelligence specialist for U.S. Navy (Active/Reserve) and Dept. of Energy since 2003
- OverWatch threat hunter since 2015
- MS computer science, Naval Postgraduate School
- Email: aaron.pickett@crowdstrike.com
OverWatch Intrusions by Threat Type
The Many Sides of Ransomware

Commodity

Big Game Hunting (BGH)

Ransomware as a Service (RaaS)
Centralized & Decentralized
Top 5 Ransomware Types in Hands-On eCrime Intrusions

- Dharma
- REvil
- Medusa
- Locker
- Phobos
- Makop
Dharma Ransomware

- Decentralized RaaS model
- Most popular ransomware of choice as observed by OverWatch
- Affiliates often use consistent techniques
- Targeting is often opportunistic
A “Typical” Dharma Intrusion (Pre-Execution)

Initial Access
- Brute forcing
- Buying stolen credentials

Defense Evasion
- Blocking users
- Disabling security

Discovery
- Security software discovery
- Scanning (internal/external)

Credential Access
- Cred dumping
- Credentials in files

Lateral Movement
- RDP
- Windows shares
What to Hunt for:

- Brute forcing via RDP and SMB
- Common/shared preparatory tools, particularly in combination with each other
  - See those listed in our blog post
- Security software discovery
- Attempts to disable security tools
  - e.g., unexpected processes interacting with security software
- Unexpected grandparent processes of discovery commands
  - e.g., Explorer, PowerShell

Thank You

We look forward to your input to help us continue to make Fal.Con better year after year.

Please fill out the survey at the link below and provide your feedback – you will be entered to win $300 on items from the CrowdStrike Swag Store!