CrowdCasts Monthly: You Have an Adversary Problem

Archived: 2026-04-06 03:14:53 UTC

- 1.
- 2.

  @CROWDSTRIKE | #CROWDCASTS AGENDA YOUHAVE AN ADVERSARY PROBLEM. 1. INTELLIGENCE-DRIVEN SECURITY 2. ADVERSARY CATEGORIZATION 3. ADVERSARY GROUPS - OVERVIEW 4. NOTABLE ACTIVITY – Q3 5. NEW ACTORS 6. ACTIONALIZING INTELLIGENCE 2013 CrowdStrike, Inc. All rights reserved. 2

- 3.

  @CROWDSTRIKE | #CROWDCASTS Today's Speakers ADAM MEYERS | VP, INTELLIGENCE Recognized speaker, trainer, and intelligence expert with 15+ years of cyber security industry experience 10 years in the DIB supporting US GOV customers on topics ranging from wireless, pen testing, IR, and malware analysis @ADAM_CYBER 2013 Crowdstrike, Inc. All rights reserved. 3

- 4.

  @CROWDSTRIKE | #CROWDCASTS Today's Speakers MATT DAHL | SENIOR ANALYST/ LEGAL COUNSEL Cyber threat analyst focused on targeted intrusion activity Focused on investigating indicators of compromise to identify specific adversary activity Legal liaison to the CrowdStrike Intelligence Team @CROWDSTRIKE 2013 Crowdstrike, Inc. All rights reserved. 4

- 5.

  @CROWDSTRIKE | #CROWDCASTS Adversaries are humans Targeted Attackers: WHO ARE THE ADVERSARIES? Motivation can range from disruption, theft, to even destruction They need to get in They will likely need to move laterally Spray and Pray (Prey): They don't care who they target (sometimes what) The more they compromise the more they win Motivation can range from disruption, theft, to even destruction 2013 Crowdstrike, Inc. All rights reserved. 5

- 6.
- 7.

  @CROWDSTRIKE | #CROWDCASTS Adversary Categorization CATEGORIZATION| Adversary Groups 1 Tactics, Techniques, and Practices 2 Never assume relationships exist Between indicators 3 Recognize adversaries are constantly changing 4 But RECOGNIZE they are HUMAN CATEGORIZATION 2013 Crowdstrike, Inc. All rights reserved. 7

- 8.

Intelligence: Adversary Groups @CROWDSTRIKE| #CROWDCASTS CHINA Anchor Panda Comment Panda Impersonating Panda Temper Panda Keyhole Panda Aurora Panda Stone Panda Vixen Panda Union Panda Poisonous Panda Pirate Panda Dagger Panda Violin Panda Putter Panda Test Panda Gibberish Panda Electric Panda Wet Panda Karma Panda Dynamite Panda Radio Panda Samurai Panda Toxic Panda Numbered Panda Pitty Panda Foxy Panda Deep Panda 2013 CrowdStrike, Inc. All rights reserved. 8

- 9.

  Intelligence @CROWDSTRIKE | #CROWDCASTS AdversaryGroups IRAN Clever Kitten: Energy Companies Cutting Kitten: For Hire NORTH KOREA Silent Chollima: Energy Companies RUSSIA Energetic Bear: Oil and Gas Companies INDIA Viceroy Tiger Government, Legal, Financial, Media, Telecom 2013 CrowdStrike, Inc. All rights reserved. 9

- 10.

  Intelligence @CROWDSTRIKE | #CROWDCASTS AdversaryGroups HACKTIVIST/ACTIVIST/ TERRORIST CRIMINAL Deadeye Jackal Commercial, Singing Spider Commercial, Financial Financial, Media, Social Networking Union Spider Manufacturing Ghost Jackal Commercial, Energy, Andromeda Spider Numerous Financial Corsair Jackal Commercial, Technology, Financial, Energy Extreme Jackal Military, Government 2013 CrowdStrike, Inc. All rights reserved. 10

- 11.

  @CROWDSTRIKE | #CROWDCASTS NotableActivity – Q3 NEW ADVERSARIES STONE PANDA | NIGHTSHADE PANDA | GOBLIN PANDA | CORSAIR JACKAL NOTABLE ACTIVITY DEADEYE JACKAL | NUMBERED PANDA | SILENT CHOLLIMA 2013 Crowdstrike, Inc. All rights reserved. 11

- 12.
- 13.

  Intelligence: STONE PANDA OPERATIONAL WINDOW May2010 to Present @CROWDSTRIKE | #CROWDCASTS TARGETING Healthcare Defense Aerospace OBJECTIVES Recon Lateral movement Data exfiltration Government TOOLS Poison Ivy RAT IEChecker/EvilGrab 2013 CrowdStrike, Inc. All rights reserved. 13

- 14.

  @CROWDSTRIKE | #CROWDCASTS TargetSectors: Healthcare, Defense, Aerospace, Government Delivery: Likely spearphishing WHO IS STONE PANDA? Malware: Poison Ivy and EvilGrab/ IEChecker Known Poison Ivy passwords: menuPass, happyyongzi, Thanksss, Xgstone, keaidestone, and admin C2 Indicators: fbi.sexxxy.biz; u1.FartIT.com; jj.mysecondarydns.com; 54.241.13.219; 184.169.176.71; 114.80.96.8 2013 Crowdstrike, Inc. All rights reserved. 14

- 15.

  Intelligence: NIGHTSHADE PANDA OPERATIONAL WINDOW Feb2008 to Present OBJECTIVES Recon Lateral movement Data exfiltration @CROWDSTRIKE | #CROWDCASTS TARGETING Media

NGO/Int'l Relations Universities TOOLS Poison Ivy PlugX 2013 CrowdStrike, Inc. All rights reserved. 15

- 16.

  @CROWDSTRIKE | #CROWDCASTS TargetSectors: Media; NGO/Int'l Relations; Universities WHO IS NIGHTSHADE PANDA? Delivery: Likely spearphishing Malware: PlugX and Poison Ivy Known Poison Ivy passwords: synnia C2 Indicators: www.adv138mail.com; pu.flowershow.org; tech.network-sec.net; 184.105.178.83; 199.59.243.106; 112.137.162.151 2013 Crowdstrike, Inc. All rights reserved. 16

- 17.

  Intelligence: GOBLIN PANDA OPERATIONAL WINDOW July2012 to July 2013 OBJECTIVES Recon Lateral movement Data exfiltration @CROWDSTRIKE | #CROWDCASTS TARGETING Aerospace Defense Energy Government Shipping TOOLS Technology Spearphishing using office doc ZeGhost specific mutexes 2013 CrowdStrike, Inc. All rights reserved. 17

- 18.

  @CROWDSTRIKE | #CROWDCASTS TargetSectors: Aerospace; Defense; Energy; Government; Shipping; Technology; Telecommunications WHO IS GOBLIN PANDA? Delivery: Spearphishing Malware: HttpTunnel (AV detection = Zegost) Mutexes: HttpTunnel@@ or Http@@@ C2 Indicators: vnpt.conimes.com; mofa.conimes.com; pvep.scvhosts.com; 112.175.79.55; 223.26.55.122; 198.100.97.245 2013 Crowdstrike, Inc. All rights reserved. 18

- 19.

  @CROWDSTRIKE | #CROWDCASTS Intelligence:CORSAIR JACKAL OPERATIONAL WINDOW February 2013 to May 2013 OBJECTIVES Information Disclosure TARGETING Energy Financial Government Shipping Telecom TOOLS Cross Site Scripting (XSS) 2013 CrowdStrike, Inc. All rights reserved. 19

- 20.

  @CROWDSTRIKE | #CROWDCASTS Timeline:CORSAIR JACKAL 2012 XTnR3v0LT colludes with Anonymous group XL3gi0n January 25, 2013 New members added January 22, 2013 XTnR3v0LT announce formation of TCA March 1 2013 Announced compromise of US financial February 2013 Announced participation in #opblacksummer July 29 2013 Ben Khlifa announces new personal page May 7, 2013 XTnR3v0LT arrested by Tunisian Authorities September 2, 2013 Tweets XSS vulnerability on Sourceforge 2013 CrowdStrike, Inc. All rights reserved. 20

- 21.

  @CROWDSTRIKE | #CROWDCASTS TargetSectors: Energy; Financial; Government; Shipping; Telecommunications WHO IS CORSAIR JACKAL? Primarily One Individual: Fahmi Ben Khlifa (XTnR3v0LT) Professed nationalistic motivations for malicious activity, but also white hat activity. Cross-site scripting attacks used to compromise databases at target organizations. 2013 Crowdstrike, Inc. All rights reserved. 21

- 22.
- 23.

  @CROWDSTRIKE | #CROWDCASTS Intelligence:DEADEYE JACKAL OPERATIONAL WINDOW TARGETING May 2011 to Present Financial Institution Media/News Social Network Platforms OBJECTIVES Propaganda Disinformation Disruption TOOLS Spearphishing Web Exploitation Facebook Spamming 2013 CrowdStrike, Inc. All rights reserved. 23

- 24.

  @CROWDSTRIKE | #CROWDCASTS Timeline:DEADEYE JACKAL August 26, 2011 May 5, 2011 SEA Mohammad Ahmad Fall 2011 – Spring 2013 Officially Formed Kabbani Killed Web Defacements Facebook Spamming September 2011 Harvard Defacement July 2013 3rd Party Provider Breaches February 2013 Twitter Account Takeovers August 2013 Domain Hijacking 2013 CrowdStrike, Inc. All rights reserved. 24

- 25.

  @CROWDSTRIKE | #CROWDCASTS TargetSectors: Financial Institutions; Media/News; Social Network Platforms WHO IS DEADEYE JACKAL? Delivery: Spearphishing Nationalistic, pro-Syrian regime motivations Defacement, account takeover, third-party provider attacks, credential collection 2013 Crowdstrike, Inc. All rights reserved. 25

- 26.

  Intelligence: NUMBERED PANDA OPERATIONAL WINDOW 2009- Present OBJECTIVES Recon Lateral movement Data exfiltration @CROWDSTRIKE | #CROWDCASTS TARGETING Government Financial Telecom Technology Media TOOLS Spearphishing Dynamic Calculation 2013 CrowdStrike, Inc. All rights reserved. 26

- 27.

  @CROWDSTRIKE | #CROWDCASTS TargetSectors: Government; Financial; Telecommunications; Media WHO IS NUMBERED PANDA? Delivery: Spearphishing Malware: Ixeshe, Mswab, Gh0st, ShowNews, 3001 C2 Indicators: getfresh.dnsrd.com; serial.ddns.ms; gfans.onmypc.us; 23.19.122.202; 192.154.108.10; 192.154.111.200 2013 Crowdstrike, Inc. All rights reserved. 27

- 28.

  Intelligence: SILENT CHOLLIMA OPERATIONAL WINDOW 2007to Present @CROWDSTRIKE | #CROWDCASTS TARGETING Multiple targets in ROK Global Targets of Opportunity OBJECTIVES Recon Criminal Monetization Lateral movement Data Destruction TOOLS Custom Malware 2013 CrowdStrike, Inc. All rights reserved. 28

- 29.

@CROWDSTRIKE | #CROWDCASTS TargetSectors: Media WHO IS SILENT CHOLLIMA? Delivery: Spearphishing Malware: HTTP/IRC-based; Tdrop; Concealment Troy; LSG C2 indicators: www.designface.net; www.sdmp.kr; www.socrates.tw; 202.172.28.111; 63.115.31.15; 209.137.232.3 2013 Crowdstrike, Inc. All rights reserved. 29

- 30.

  @CROWDSTRIKE | #CROWDCASTS INTELLIGENCE-DRIVENSECURITY INTELLIGENCE| Adversary-Centric 1 INTELLIGENCE Understand the adversaries targeting your Vertical | Company | Geo-Location | Customers 2 Build appropriate defenses to counter/detect these adversaries 3 Perform other security practices from an Adversary-centric perspective Pen Testing (Red Team) Security Operations Briefings Log Review 2013 Crowdstrike, Inc. All rights reserved. 30

- 31.

  @CROWDSTRIKE | #CROWDCASTS INTELLIGENCE-DRIVENSECURITY INTELLIGENCE| Making it Actionable 1 ACTIONALIZING INTELLIGENCE Intelligence is difficult to consume Lots of information to keep straight New data constantly flowing in (possibly unvetted) 2 Security Operations need to change shi s & people 3 Actionable Intelligence Pass down can’t possibly occur with all indicators 2013 Crowdstrike, Inc. All rights reserved. 31

- 32.

  @CROWDSTRIKE | #CROWDCASTS AdversaryMicrosite COMING SOON TRACK: Track current Adversaries against other Industry nomenclature OVERVIEW: Gain insight Into adversary – new groups Added weekly 2013 Crowdstrike, Inc. All rights reserved. 32

- 33.

  @CROWDSTRIKE | #CROWDCASTS RESOURCES Nextup: Enterprise Activity Monitoring The Power to HUNT November 5th | 2PM ET/11AM PT Download a Sample Adversary Intelligence Report http://www.crowdstrike.com/ sites/default/files/deeppanda.pdf For additional information, CONTACT SALES@CROWDSTRIKE.COM *NEW* Videos Every Thursday | 1PM ET http://www.crowdstrike.com/crowdcasts/index.html 2013 Crowdstrike, Inc. All rights reserved. 33

- 34.

  Q&A Q&A @CROWDSTRIKE | #CROWDCASTS Pleasetype all questions into the Q&A section of the GoToWebinar Control Panel If you have additional ?’s, contact us At crowdcasts@crowdstrike.com 2013 CrowdStrike, Inc. All rights reserved. 34
