No Easy Breach DerbyCon 2016

Archived: 2026-04-05 13:41:38 UTC

- 1.

  1 NO EASY BREACH DERBYCON 2016 #NOEASYBREACH Matt Dunwoody @matthewdunwoody Nick Carr @itsreallynick

- 2.

  2 How It All Started • 1 average spearphishing email • 1 failed client remediation • 1 very determined nation state • Attacker’s mission not impacted by ongoing remediation measures • 2 attacker objectives: • Steal email of targeted VIPs • Monitor security team, response & detection efforts FUN FACT: This was APT29

- 3.

  3 Several Months Later… • The Aftermath • Four person Mandiant team • Over 1,039 compromised systems • Over 1,000 unique malware samples • Over 1,000 different unique C2 domains / IPs • Over 50,000 email communications stolen • Including scripts & tools: 7,000+ attacker files • How did they pull it off? • Fast-paced intrusion • Very stealthy • Rapidly changing tactics • Employed advanced attack techniques

- 4.

  4 Challenge 1: Fast-Paced Attacker • Attacker infected 10 systems per day with primary backdoor family • Especially when provoked (maintained baseline foothold) • Accessed hundreds of systems for recon and credential theft • Removed tools and forensic artifacts to hide activity • Deployed additional backdoor families • Continued to steal data every week

- 5.

  5 Our Response: Triaged Where Possible • Moved from typical Live Response analysis to abbreviated triage • Brief analysis leveraging known attacker TTPs • Developed indicators to assist triage • Partially automated the analysis process • Some activity not unique enough to sig • Focused on: • Lateral movement • Walking back up the chain • Pivoting, recon, new tools or backdoors • Signs of data theft • Deviation from typical attacker activity FAST-PACED ATTACKER

- 6.

  6 Our Response: Streamlined Documentation • Typical LR reports and timelines took too much time • Still needed to document findings • Compressed notes from systems into brief, standardized text blocks • Malware and attacker tools on the system • Persistence mechanisms • Periods of

attacker activity and significant timestamps • Source of activity • Documented significant findings • New TTPs • Data theft FAST-PACED ATTACKER

- 7.

  7 Lesson Learned: Be Fast and Flexible • Be willing to change normal practices and disregard official methodologies when they're not working • Make the most of outside help - accept the limitations of your circumstances and do what you can to maximize your chances of success FAST-PACED ATTACKER

- 8.

  8 Challenge 2: Stealthy Attacker • Attacker using counter forensic techniques to hide endpoint and network activity • Endpoint: secure deletion, impressive OPSEC (pack up and move), 90% doctrine • Network: compromised third party websites & social media C2, altered communication scheme + strong crypto, embraced SSL • The odds were stacked against us • Unable to use Mandiant network sensors and signatures • Existing devices inconsistently-deployed and coverage spotty • "Rolling remediation" actions showed our hand so attacker knew which evasion tactics were working

- 9.

  9 • Attacker considered every detail • Mass activity to obscure the real target • More evident in recent campaigns • Widespread phishing with a prioritized target list • They might even want the first system to be caught • Data theft using only legitimate US-based services, complicating any law enforcement response • Gmail, Google Drive using APIs • OneDrive • Monitored Us • Targeted the IR operations throughout the compromise • Were we onto them and how much time did they have left? BONUS SLIDE: Even More OPSEC he looks cozy

- 10.

  10 Our Response: Found Clues in the Ruble • Maximized the utility of trace forensic artifacts • Some attacker behavior recovered from sdelete • File path regex for artifacts • Everything from AAA.AAA to ZZZ.ZZZ • Entry Modified timestamp typically indicated when sdelete occurred • EULA Accept registry key for each Sysinternals tool • Searched for new sdelete usage • Prefetch entries for some operations (e.g., RAR) included deleted items in Accessed Files STEALTHYATTACKER FUN FACT: Now it's built-in!

- 11.

  11 Our Response: Made the Best of What We Had • Learned and leveraged client's network tools • Embraced the varying technology across business units • Took time and patience to filter out the network noise • Searched for every new system by timeframe • Searched activity between sets of infected hosts • Automated where possible • Developed dashboards STEALTHYATTACKER

- 12.

12 Our Response: Made the Best of What We Had • Found the helpful but forgotten alerts • SMB transfer of UPX-packed files • Extracted fields we wanted • Signature combinations solved mysteries • Schtasks.exe usage by UUID • SMB writes to System32 • Network time preserved when other timestamps could not be trusted STEALTHYATTACKER signature=MSRPC_SuspiciousEncryption event_info="UUID=86d35949-83c9-4044-b424- db363231fd0c*" src_ip="10.*" dest_ip="10.*" (dest_port=49154 OR dest_port=49155) FUN FACT: This was our initial discovery of HAMMERTOSS

- 13.

13 Our Response: Made New Shiny Things • Deployed additional budget-friendly open source tech • Found ways to apply our methodology • Connected to our incident tracker • Sparklines for time + volume of activity • Prioritized host analysis based on traffic • Smashed and grabbed before the wipe! STEALTHYATTACKER host_10 host_9 host_8 host_7 host_6 host_5 host_4 host_3 host_2 host_1

- 14.

14 Lesson Learned: Improve Visibility and Don’t Stop Looking • Map attacker activity to potential data sources and use everything available to minimize blind spots • Give your team access to existing tools outside of their normal process • Consider deploying additional technology • Network time provides reliable chronology despite host-based timestomping • Combat IR fatigue by automating high-confidence (and boring stuff) • Once an attacker is found, fight to maintain line-of- sight STEALTHYATTACKER

- 15.

15 Challenge 3: Rapidly-Evolving Tactics • New and updated backdoors • 7 distinct backdoor families • SEADADDY went through 3 version updates • Seven unique persistence mechanisms • Registry run key, .LNK files, services, WMI, named scheduled tasks, hijacking scheduled tasks, over-writing legitimate files • Cycled persistence techniques regularly • Minimal re-use of metadata commonly tracked and shared as indicators • Malware MD5, file name, file size, and C2 unique to each system • Attacker didn’t need to re-use compromised accounts FUN FACT: On current case, APT29 used unique UAC bypass & persistence that was first posted online days before

- 16.

16 Our Response: Maintained Eye Contact • Fought to keep network visibility on all malware families • Backdoor version 1: could see it, sig it, and decode it PHPSESSID = base64(zlib(aes(BACKDOOR C2))) • Backdoor version 2: lost ability to decode it Cookie{2,7} = custom64(zlib(rc4(aes(BACKDOOR C2)))) • Backdoor version 3: lost ability to sig it random_split(Cookie{2,7} = custom64(zlib(rc4(aes(BACKDOOR C2)))) • Wrapped in SSL: lost ability to see it … at first RAPIDLY-EVOLVING TACTICS FUN FACT: This was SEADADDY certificate email SSL cipher start stop root@domain1.com TLS_DHE_RSA_WITH_AES_256_CBC_SHA 10/14/15 14:13:00 10/15/15 00:14:37 support@vendor.com TLS_RSA_WITH_3DES_EDE_CBC_SHA 10/14/15 16:13:29 10/14/15 16:13:29 root@domain2.com TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 10/13/15 13:30:17 10/14/15 03:14:04

admin@example.com TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA 10/11/15 13:02:21 10/12/15 10:58:59 Finding attacker SSL usage using Bro's ssl.log

- 17.

  Copyright © FireEye,Inc. All rights reserved.17 Our Response: Prioritized the Unknown • Spent time analyzing systems with unknown activity • The most interesting systems were the ones accessed but we didn't know what they did • Limited analysis on systems with known and consistent attacker tactics • While not useful as standalone indicators, tracked breach data to prioritize discovered systems • Identified common forensic artifacts between systems with shared C2 RAPIDLY-EVOLVING TACTICS

- 18.

  Copyright © FireEye,Inc. All rights reserved.18 Our Response: Continually Improved Indicators • Created indicators for every stage of attack lifecycle • All seven persistence mechanisms, recon, lateral movement, and data theft • Methodology IOCs helped identify systems without known malware • Reverse engineered every backdoor revision & updated indicators • Maintained a list of high-confidence indicators to focus new IOC development • Developed flexible & resilient indicators • Provided high-fidelity matches across versions, regardless of morphing • Used imports and exports, size ranges, section names, compile times, and other consistent attributes RAPIDLY-EVOLVING TACTICS

- 19.

  Copyright © FireEye,Inc. All rights reserved.19 Our Response: Continually Improved Indicators RAPIDLY-EVOLVING TACTICS • Automated analysis of backdoor for comparison and configuration extraction; enterprise-wide search of process memory • Indicators based on packaging and delivery • Import hashes, size, section names, artifacts of wrapper execution everywhere possible • Adapted file system IOC+regex to process handles, prefetch, and event logs • Identified malware staged for SMB transfer obfuscated- backdoor.py PyInstaller / Py2Exe UPX-packed ...transferred laterally

- 20.

  Copyright © FireEye,Inc. All rights reserved.20 Lesson Learned: Find It, Refine It, Re-Find It • Enhance and test your best indicators even when they're working • Track what the attacker can change before you lose visibility of their activity • Don't let technical data fall through the cracks, even when visibility is good and the details have marginal value as indicators RAPIDLY-EVOLVING TACTICS

- 21.

  Copyright © FireEye,Inc. All rights reserved.21 Challenge 4: Advanced Attack Techniques • Windows Management Instrumentation (WMI) • Attacker used WMI to persist backdoors • Embedded backdoor files and PowerShell scripts in WMI repo • Used WMI to steal credentials from remote systems • Configured WMI to extract and execute backdoors months in the future, to evade remediation • Attacker leveraged PowerShell • Stealthy backdoors • PowerShell scripts like Invoke-Mimikatz evaded A/V detection • Excellent WMI integration • Kerberos • Attacker used Kerberos ticket attacks, which made tracking lateral movement difficult

- 22.

  22 Our Response: Tackled Attacker WMI Usage • Searched for WMI persistence • Manually parsed from objects.data strings on endpoints • Ran script across the environment to identify persistence • Colleagues developed custom MIR audit to allow for sweeping • Identified evidence of attacker code in WMI repo • Attacker embedded PowerShell code in WMI class properties to execute on remote system • Identified class and property names and code in objects.data strings • Searched contents of CIM repo at scale • Parsed out embedded scripts and malware • The repo was a poorly documented, complex structure, so parsing was difficult and manual • Willi Ballenthin, Matt Graeber and Claudiu Teodorescu made repo parsers (after the investigation was completed) ADVANCED ATTACK TECHNIQUES

- 23.

  23 Our Response: Tackled Attacker WMI Usage ADVANCED ATTACK TECHNIQUES

- 24.

  24 Our Response: Increased PowerShell Visibility • Upgraded the environment to PowerShell 3.0 and enabled logging • Logging captured input/output, variable initialization, etc. • Captured entire functions of PS scripts, attacker commands, script output, etc. • Wrote indicators based on observed attacker activity • Identified lateral movement, unique backdoors, credential theft, data theft, recon, persistence creation, etc. • Turned attacker PowerShell usage from a threat to a benefit • Logging and IOCs made finding and analyzing attacker activity much easier ADVANCED ATTACK TECHNIQUES FUN FACT: There's now a blog post and my script block logging parser on GitHub

- 25.

  25 Our Response: Increased PowerShell Visibility ADVANCED ATTACK TECHNIQUES

- 26.

  26 Our Response: Addressed Ticket Attacks • Worked around Kerberos attacks • Swept for Invoke-Mimikatz PTT usage in PS logs to identify pivot systems • Swept for other indicators of lateral movement to identify destination systems • Looked for remote Kerberos logons around the time of attacker activity • Developed indicators • Based on research by Sean Metcalf at adsecurity.org • Developed late in the investigation • Extremely high-fidelity ADVANCED ATTACK TECHNIQUES

- 27.

  27 Our Response: Addressed Ticket Attacks ADVANCED ATTACK TECHNIQUES Event ID 4624 Event ID 4672 Event ID 4634

- 28.
- 29.

Inc. All rights reserved.29 BONUS SLIDE: Even More WMI + PS FUN FACT: We saw the attacker test this backdoor before deployment

- 30.

  Inc. All rights reserved.30 Lesson Learned: Turn Weakness Into Strength RAPIDLY-EVOLVING TACTICS • Use attackers' strengths against them • Unique attacks make for high-fidelity indicators • Identify the activity • Develop indicators • Increase visibility at scale • Automate detection • Create an alerting system, if possible

- 31.

  Inc. All rights reserved.31 • Backdoor used TOR hidden services to provide secure, discrete remote access • Used Meek plugin to hide traffic • Forwarded TOR traffic to ports: • 3389 – Remote Desktop • 139 – Netbios • 445 – SMB • Modified registry to enable RDP • "Sticky-keys" to provide unauthenticated, privileged console access BONUS SLIDE: TOR backdoor (just because it's cool) FUN FACT: This was first deployed 3 hours before remediation

- 32.

  Inc. All rights reserved.32 BONUS SLIDE: TOR backdoor (just because it's cool)

- 33.

  Inc. All rights reserved.33 BONUS SLIDE: TOR backdoor (just because it's cool) Client Endpoint APT29 (actual image) TOR network Meekreflector .appspot.com Mail.google.com Google Cloud SSL HTTP TOR TOR

- 34.

  Inc. All rights reserved.34 If You've Learned Nothing Else Today… SUPER IMPRESSIVE CONCLUSION SLIDE • You must match or exceed the attacker's pace • You must match or exceed the attacker's visibility • You must match or exceed the attacker's development • You must match or exceed the attacker's advanced techniques • You must match or exceed the attacker's intensity.

- 35.

  Inc. All rights reserved.35 "True happiness incident response is a life of continual self-improvement. The greater the struggle, the more enriching the experience is for your life."

- 36.

  Inc. All rights reserved.36 THANK YOU QUESTIONS? DERBYCON 2016 #NOEASYBREACH Matt Dunwoody @matthewdunwoody Nick Carr @itsreallynick

---