Module 2: Incident Detection Report

Kyler Kent

School of Continuing Studies, Georgetown University

MPCR-6780-101: Cyber Surveillance Operation & Legal Framework

Dr. Rosemarie Pelletier

September 10, 2023

Module 2: Incident Detection Report

Dear CISO:

To successfully monitor the attack, Ackme should monitor for the key IOC, which was “split HTTP post requests” with “two account numbers” present, indicating the exfiltration and billing redirection activity (Thexpert, 2019, 02:30-02:32). Ackme does not appear to be monitoring HTTP requests from Badger AMR systems. Therefore, several monitoring configuration options are available. First, a network TAP could be placed between the Badger AMR systems and the LAN/Ethernet connection to monitor traffic. This solution may be costly as a TAP would need to be provided for each Badger AMR system, which are very diffuse. A TAP could cost $229 per unit (Dualcomm, n.d.). With the total number of Badger AMR systems at approximately 20,000, the price of this solution comes out to approximately $4.5 million without central monitoring accounted for. Some benefits are very obvious, including direct monitoring of inbound/outbound traffic from the Badger AMR units. Due to the expense, I recommend we sample and randomly choose Badger AMR systems to tap for randomized monitoring and threat hunting rather than widespread monitoring unless our business risk elevates and we believe we are under another attack. Additionally, port mirroring could be configured on each Badger AMR system’s existing switch to forward packets to a monitoring port at no extra cost, as each switch has the capability of port mirroring at least the uplink. The monitoring ports could be aggregated as multiple NICs via a tool like Wireshark, with a filter set containing regex to look for split HTTP post requests and multiple billing account numbers (Wireshark Wiki, 2022; Wireshark, n.d.). Additionally, a script via SSH admin access could be configured on each switch or router to forward port mirroring to a central server or SIEM, which also has a script to import the packet capture to an SIEM such as Splunk. Once the data is ingested into Splunk, an SIEM rule can run with logic similar to the Wireshark filter to look for the IOCs (i.e., split HTTP post requests and multiple billing accounts) (Splunk, n.d.). It can alert directly to our cybersecurity analysts for investigation and confirmation. Therefore, there are both manual and automated approaches to this situation. A drawback of the router and switch solution could be that not all switches support multi-port mirroring and may only be able to mirror the uplink, potentially missing LAN activity not destined for the Internet or back. Finally, as a point of improvement for our operations and our continuous monitoring effort, we could consider a 100 GBPS packet capture 1U server such as the one from FMADIO to centrally ingest high throughput packet capture from all network areas and process for both central manual and automated analysis (FMADIO, 2023). We spoke with the supplier for FMADIO and they stated that the cost would be approximately $5,000 for each 1U server. Our network security engineers estimate we need at least 20 of these devices (one per geographic area of operation), making the total cost of this deployment/solution $100,000, which is more than economical to process continuous packet capture. A final solution could be the FMADIO 1GBPS 1U servers and a combination of switch or router port mirroring (as the Badger AMR systems could be on an Ethernet or wireless network (Georgetown University, 2020, pp. 4-5)) to the FMADIO 1U server. This configuration would also appropriately represent our current risk levels to support our continuous monitoring needs while balancing the budget in the wake of an active incident response effort and potential data breach. Changes will be made to forward to our existing Splunk instance at no extra cost. Additionally, as we discuss below, packet capture will be indispensable for activities other than post-incident response, such as threat hunting to proactively detect another cyber breach like this one.

Once the firmware is rolled back to the non-vulnerable state, Ackme should proceed to do a substantial hardware, software, and security risk assessment of all assets, including third-party assets. Additionally, a substantial supply chain risk assessment should take place to identify more supplier risks to prevent a similar disaster from occurring like from CI Company. Another activity that should take place is the employment and deployment of Cyber Threat Hunters to seek out IOCs before breaches are detected. Threat-hunting activities should include the use of randomized packet capture and analysis of any and all network assets and communications. Furthermore, after analyzing CI Company's breach disclosure, Ackme should include in its architectural requirements for all assets to include a hardware Root of Trust and Chain of Trust as described in NIST SP 800-193 (Regenscheid, 2018, p. 11). Hardware devices should include, among other items and requirements, a TPM (Trusted Platform Module) to help provide secure attestations about device firmware and software (Regenscheid, 2018, pp. 4-5). Devices should include OS (operating system) architectural requirements that include "Secure Boot" where a TPM will be used to cryptographically validate the firmware version and configuration and will not allow the system to boot with any unsigned or unauthorized changes or modifications (Regenscheid, 2018, p. 8; Souppaya et al., 2017, p. 28). Secure Boot will act as a strong preventative control against further supply chain or firmware backdoor placement activities.

As stated before, sufficient plans have been made to move forward and secure Ackme from our emerging cyber threats. These would also limit the scope of damage of future attacks, as continuous monitoring at the endpoint (i.e., Badger AMR system) would allow the future detection of backdoors of this nature. Therefore, detection and incident response could occur within days instead of months, potentially confining a compromise to a small geographic area. Furthermore, the use of secure remote management protocols such as SNMPv3 and SSH to remote administer routers and switches could also be used to quarantine LANs when a compromise is suspected by disabling an uplink and still allowing port mirroring of potentially other ports for continuous monitoring. This would prevent potential lateral movement from each Badger AMR system, which was a persistent motif during the breach disclosure (Georgetown University, n.d., para. 1). Next, privilege access management (PAM) on root administrators would be our next step. Even though CI Company was primarily the victim of the phishing attack, Ackme can still learn from their initial access and initial compromise and develop additional controls to limit the scope of a similar attack (Georgetown University, n.d., para. 1). Requiring MFA is a possibility via an MFA token for root administrators on the Badger AMR system. This would prevent the use of harvested credentials from phishing without a second factor of authentication that would be much more difficult to obtain. Furthermore, a robust Zero-Trust Network architecture could “limit internal lateral movement” per NIST SP 800-207 (Borchett et al., 2020, p. 1). Whereas typically a domain admin could be granted access to any resource via a single-sign-on method such as Kerberos, a Zero-Trust Architecture would constantly limit access to resources and require secondary checks, such as MFA challenges before granting additional access. Furthermore, least privilege could also have been configured on the domain admins to limit access, such as write access to CI Company’s crown jewels (i.e., custom-coded firmware for their Badger AMR systems), via a method such as M of N control (Sunflower-CISSP.com, n.d.). By requiring a minimum number of administrators to approve and move firmware code into production, a single domain admin account compromise could not perform the task of injecting a backdoor into production firmware. Finally, a robust user awareness training program could have vastly limited the number of administrators who fell victim to the attack. Furthermore, a robust phishing email reporting system could have also flagged the email and helped uncover the initial access of the compromised admins who fell victim to the phishing attempt.

If the above controls are implemented for Ackme, our risk is very limited if attackers already have access to the network or have Badger AMR backdoor access prior to rollback. Network access would be limited because Zero-Trust architecture and firmware backdoor placement would also be very difficult with M of N control. Additionally, continuous admin MFA checks would seriously limit credential harvesting and lateral movement. Finally, if backdoor access is established to Badger AMR systems, we would have substantial detective controls in place with the example FMADIO 1GBPS 1U servers and streamed packet capture from network switches and routers. We would quickly detect indicators of compromise from a backdoor exploit and be able to start responding to compromised Badger AMR systems. Even a Secure Boot architecture with a hardware Root of Trust would stop the boot of Badger AMR systems even if the firmware backdoor was installed. However, if Ackme was placed in this scenario with our current controls, our corresponding risk would be very high, and our business would not be sustainable due to threats like domain-wide admin takeover and the high possibility of persistence from the attackers. Additionally, due to the billing siphoning activity, we would incur a significant financial penalty.

Finally, to properly assess the scope of the damage, incident response efforts will need to account for the total dollar amounts siphoned out to the rogue financial accounts, as that was the primary motive of the threat actor (Thexpert, 2019, 2:14-2:45). This will help enumerate the direct financial impact of the cyber incident. Additionally, incident response teams will need to monitor man-hours to determine how much time is taken to restore Badger AMR systems to non-vulnerable firmware versions. Thus, direct and indirect costs should be assessed to calculate damages from the cyber incident. By utilizing existing security controls, like continuous monitoring of servers and network appliances, Ackme can help monitor and detect if the attack on CI Company moved beyond to Ackme servers, network infrastructure, or Ackme user accounts. Therefore, Ackme will need to remain in a high state of alert and vigilance with its security operations team until the incident response is confirmed to have ended. Furthermore, Ackme will need to work towards deploying packet capture on other areas of the network to detect similar malicious activity in HTTP and other application-layer protocols. Thus, this incident is a great opportunity for Ackme to improve its security posture and rise to the challenge of emerging cyber threats.

References

Borchett, O., Connelly, S., Mitchell, S., & Rose, S. (2020). Zero Trust Architecture. In *NIST.gov* (NIST Special Publication 800-207). NIST Technical Series Publications. Retrieved September 10, 2023, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf?TB_iframe=true&width=370.8&height=658.8

Dualcomm. (n.d.). *Amazon.com: Dualcomm ETAP-2003 10/100/1000Base-T Gigabit Ethernet Network TAP : Electronics*. Amazon. Retrieved September 10, 2023, from https://www.amazon.com/gp/product/B004EWVFAY/ref=ppx_yo_dt_b_search_asin_title?ie=UTF8&psc=1

FMADIO. (2023). *FMADIO100 - 100Gbps Packet Capture — FMADIO*. Retrieved September 9, 2023, from https://www.fmad.io/100g-packet-capture

Georgetown University. (n.d.). CONFIDENTIAL PARTNER DISCLOSURE. In *Georgetown University Canvas*. School of Continuing Studies. Retrieved September 7, 2023, from https://georgetown.instructure.com/courses/175977/pages/module-2-response-to-a-spear-phishing-attack?module_item_id=3283355

Georgetown University. (2020). H. Ackme Oil & Gas Background Material. In *Google Drive*. Retrieved September 7, 2023, from https://drive.google.com/file/d/1TDoFQQWPZTgWTncVxTrKOfP2rMGkz_Re/view

Regenscheid, A. (2018). Platform Firmware Resiliency Guidelines. In *NIST.gov* (NIST Special Publication 800-193). NIST Technical Series Publications. Retrieved January 15, 2023, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf

Splunk. (n.d.). *About Splunk regular expressions - Splunk Documentation*. SPL2 Search Manual. Retrieved September 10, 2023, from https://docs.splunk.com/Documentation/SCS/current/Search/AboutSplunkregularexpressions

Sunflower-CISSP.com. (n.d.). *M of N control - Sunflower-CISSP.com*. Retrieved September 10, 2023, from https://www.sunflower-cissp.com/glossary/cissp/3455/m-of-n-control

Thexpert, J. (2019, July 23). *Threat Briefing from Cyber Threat Analyst at Critical Infrastructure Co.* https://drive.google.com/file/d/1skFV5MPB6PqHuW8E239wrc5qP0PlEXUg/view?t=94s

Wireshark. (n.d.). *Wireshark · Display Filter Reference: Hypertext Transfer Protocol*. Wireshark.org. Retrieved September 10, 2023, from https://www.wireshark.org/docs/dfref/h/http.html

Wireshark Wiki. (2022). *DisplayFilters*. Retrieved September 10, 2023, from https://wiki.wireshark.org/DisplayFilters