Section 1: Week 3: Avoid or Control Persistent Threats

Nate Bachmeier

TIM-7030: Managing Risk, Security, and Privacy

June 21, 2020

North Central University

# Avoid or Control Persistent Threats

Malicious actors, targeted attacks, and advanced persistent threats (APT) each seek to disrupt the confidentiality, integrity, and availability of information systems. These different groups seek out their victims with varying levels of specificity and sophistication (see Table 1). After gaining access through phishing emails, an APT has established a foothold within the NCU Financial (NCU-F) network. The organization needs a strategy to remove the uninvited guests and recover control of the network. When a significant security breach occurs, and the business experiences a state of crisis, this can be a highly efficient period to enact change and strength the overall security posture (Weston, Conklin, & Drobnis, 2018). This reinforcement process needs to consider changes to people, processes, and products through the lens of Risk Management Frameworks (RMF), regulatory and ethical standards, and new Intrusion Detection and Prevention Systems (IDS/IPS).

Table 1: Classifications of Attackers

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Target Selection | Description | Sophistication |
| Generic Malicious Actor (Fischerkeller & Harknett, 2017) | Random Selection | Use automation to attack thousands of systems, exploiting attacker defender economics | Relies on the Law of Large Numbers |
| Targeted Attackers (Alshamrani A, 2019) | Specific / Short Term | Identity specific industries and business artifacts for exploitation | Relies on social engineering and other known vulnerabilities |
| Advanced Persistent Threats (Alshamrani A, 2019) | Specific / Long Term | Seeks prolonged control over a target for months to decades | Well-financed organizations with ‘state-of-the-art’ weapons |

## Risk Management Framework (RMF)

When an attacker compromises an organization, there can be a sense that discarding the RMF is the best course of action. However, most frameworks fundamentally follow the same feedback loop of ‘plan-do-act-check’ (Radhakrishnan, 2015). Instead, the business needs to assess their needs in terms of regulatory requirements, process maturity, and cultural norms (see Table 2). If the process does not align with the expectations of internal partners, then it will face political pressure and avoidance (Dunn, 2014). After considering these aspects, the NCU-F security team recommends remaining on ISO 27000, as it addresses the regulatory expectations of financial institutions. Nevertheless, the system compromise highlights that improper controls exist, and changes to the framework’s implementation are necessary.

Table 2: Risk Management Frameworks

|  |  |  |
| --- | --- | --- |
| Name | Description | Ideal Environment |
| National Institute of Standards and Technology (NIST) Cybersecurity Framework (Grohmann, 2018) | Flexible methodology to approach controls and evolve them over time | Large enterprise and businesses with varying levels of process maturity |
| International Organizational Standards (ISO) 27000 (Gillies, 2011) | Rigid set of requirements for ensuring appropriate controls | Small enterprises and heavily regulated industries |
| Control Objectives for Information and Information related Technology (COBIT) (Devos & Van de Ginste, 2015) | Collection of industry best practices and guidelines | Organizations that need a middle ground between NIST and ISO frameworks |

## Relevant Laws and Standards

During the APT’s tenure within the private network, it could have been privy to confidential information about the institution and its customers. This situation creates both regulatory and ethical expectations of publically disclosing the security incident. States like California, Delaware, and Utah have strict privacy legislation that can hold NCU-F responsible for negligence. In September 2017, Equifax announced a data breach impacting 147 million people, costing over 575 million dollars in settlements plus public relations (Puig, 2019). If the incident exposes European customer data, then the General Data Protection Regulation (GDPR) can impose additional fines (Kovacs, 2017). Even without these legal requirements, NCU-F has an ethical obligation to be forthcoming. The truth always comes out, and failing to act degrades the companies ability to drive the public narrative.

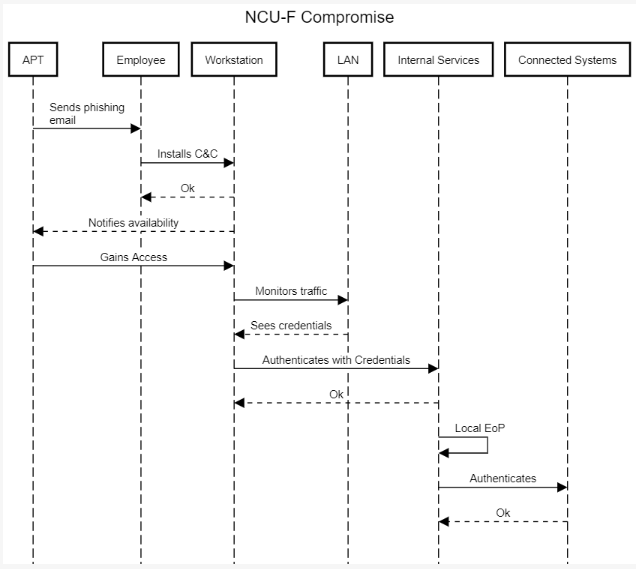
## Adopting Process

The adoption of any process requires sponsorship from executive leadership and proper communication to the troops (Weston, Conklin, & Drobnis, 2018). When either the top or bottom of the organization lack agreement in the solution, it will not become a priority, and team members will sidestep it. Instead, having a cultural alignment ensures that the standard operating procedure makes safe decisions that minimize risk and privacy concerns. For instance, NCU-F’s intrusion began with a phishing attack. Security awareness training could reduce the likelihood of that scenario but not eliminate it (Hunt, 2019). Through a similar mechanism, RSA became compromised via malicious emails, automatically triggering a zero-day exploit in Adobe Flash (Leyden, 2011). After slipping past the firewall, many enterprise environments lack defense-in-depth controls allowing lateral movement across the network (Stevens, 2018). Removing these auxiliary threats requires a fundamental shift in approach that centers around zero-trust and an assume breach mindset. Promoting such a shift is only possible under a shared vision of success and collective agreement that change is necessary.

## Changes to Operations and Services

The forensic analysis concludes that the attack against NCU-F began with malware embedded in email communications (see Figure 1). When the user interacts with the message, it provisions a command and control (C&C) service to receive commands from the attacker. These commands execute under the same security context as the local workstation, allowing actions such as monitoring network traffic to discover unprotected credentials. After discovering hashes and passwords, the breach laterally moves to internal services (e.g., file shares and repositories). Each hop across the network topology expands the APT’s control as they collect privileges to auxiliary connected systems (e.g., databases and management solutions). Recovering the system can be challenging, as the APT becomes free to install backdoors across arbitrary resources.

Figure 1: Sequence of Events



## Best Practices for Security and Risk Management

Multiple controls and policy changes are necessary to prevent these scenarios from reoccurring (see Table 3). Applying these best practices requires identifying the resources that constitute the internal network, then exploring the mechanisms for authentication, authorization, and auditing (AAA) their interactions. While it is often easy to identify a solution to preventing exploitation of a path, this can often come at odds with business priorities. Removing the email service would remove this series of unfortunate events. However, it is unrealistic for the sales and marketing department to divorce themselves from the medium. Even if a solution would possible, an attacker could launch phishing attacks against the employees’ private accounts or social media networks.

Table 3: System Improvements

|  |  |  |
| --- | --- | --- |
| Threat | Remediation | Challenges |
| Malicious email reaches the employee | Spam and anti-virus software can reduce the likelihood of success (Lee, Moon, & Park, 2017) | Completely blocking document exchange is challenging to impossible |
| Installation of C&C | Running systems with least privileges prevent success (Fischerkeller & Harknett, 2017) | Many users require dangerous permission to perform their role |
| C&C Communicates with a remote attacker | Prevent communicating with untrusted networks | Preventing access to public clouds is nearly impossible (Paller, Mahalik, Skoudis, & Ullrich, 2020) |
| The attacker steals credentials from the network | Install IPSec and use TLS encryption | Not all systems fully support these protocols |
| The attacker compromises switch ARP tables | Use static ARP tables via domain policy | Prohibitively expensive in dynamic environments |
| Attacker accesses internal services using stolen credentials | Rotate credentials frequently, use Multi-Factor Auth (MFA) (Hennig, 2018) | Does not prevent stolen hash |
| Local Elevation of Privilege on Internal Systems | Patch management and disable unused services (Galinec & Steingartner, 2017) | Difficult to schedule on mission-critical systems (Thomas & Adelwahed, 2017) |
| Attacker repeats the process to access auxiliary connected systems | Use authorization policy to limit capabilities | Not all systems fully support these restrictions |

## Software Solution Recommendations

In addition to standard solutions, such as anti-virus and patch management, the business should also consider intrusion detection systems that rely on signatures (Mehresh & Upadhyaya, 2015). These technologies confirm that the system meets cryptographical proofs that tampering has not occurred. For instance, the operating system can use a Trusted Platform Module (TPM) to confirm the integrity of the boot loader and other critical components. An argument exists for network traffic anomaly detection and HoneyPots (Westcon-Comstor, 2018). However, these tools can report false positives and be challenging to configure correctly.

# References

Alshamrani A, M. S. (2019). A survey on advanced persistent threats: techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys and Tutorials, 21*(2), 1851-1877. doi:https://doi.org/10.1109/COMST.2019.2891891

Devos, J., & Van de Ginste, K. (2015). Towards a Theoretical Foundation of IT Governance - The COBIT 5 case. *Electronic Journal of Information Systems Evaluation, 18*(2). Retrieved from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=edb&AN=109261833&site=eds-live

Dunn, M. (2014). Breaking the cyber-security dilemma: aligning security needs and removing vulnerabilities. *Science and engineering ethics, 20*(3), 701-715. doi:https://doi.org/10.1007/s11948-014-9551-y

Fischerkeller, M., & Harknett, R. (2017). Deterrence is not a credible strategy for cyberspace. *Orbis, 61*(3), 381-393. doi:https://doi.org/10.1016/j.orbis.2017.05.003

Galinec, D., & Steingartner, W. (2017). Combining cybersecurity and cyber defense to achieve cyber resilience. *14th International Scientific Conference on Informatics.* Poprad, Slovakia: Institute of Electrical and Electronics Engineers. doi:https://doi.org/10.1109/INFORMATICS.2017.8327227

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *TQM Journal, 23*(4), 367-376. doi:http://dx.doi.org.proxy1.ncu.edu/10.1108/17542731111139455

Grohmann, A. (2018). Evolution of the cybersecurity framework. *Information Systems Security Association, 16*(7), 14-18. Retrieved May 2, 2020, from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=tsh&AN=130572679&site=eds-live

Hennig, N. (2018). Privacy and Security Online: Best Practices for Cybersecurity. *Library Technology Reports, 54*(3), 1-37. Retrieved from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=ehh&AN=128707555&site=eds-live

Hunt, T. (2019). Hack to the Future. *NDC Conferences.* Minnesota: NDC. Retrieved May 9, 2020, from https://www.youtube.com/watch?v=qCOefMiakps

Kovacs, L. (2017). Cybersecurity policy and strategy in the European Union and NATO. *Revista Academiei Fortelor Terrestre, 23*(1), 16-24. Retrieved from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=a9h&AN=128789540&site=eds-live

Lee, J., Moon, S., & Park, J. (2017, July). CloudRPS: a cloud analysis based enhanced ransomware prevention system. *Journal of Supercomputing, 73*(7), 3065-3084. doi:https://doi-org.proxy1.ncu.edu/10.1007/s11227-016-1825-5

Leyden, J. (2011, April 11). *RSA explains how attackers breached its systems*. Retrieved June 21, 2020, from The Register: https://www.theregister.com/2011/04/04/rsa\_hack\_howdunnit/

Mehresh, R., & Upadhyaya, S. (2015). Surviving advanced persistent threats in a distributed environment - architecture and analysis. *Information Systems Frontiers, 17*(5), 987-997. Retrieved from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=edb&AN=109474409&site=eds-live

Paller, A., Mahalik, H., Skoudis, E., & Ullrich, J. (2020). The five most dangerous new attack techniques and how to counter them. *RSA Conference.* RSA. Retrieved May 9, 2020, from https://youtu.be/xz7IFVJf3Lk

Puig, A. (2019). *Equifax Data Breach Settlement: What You Should Know*. Retrieved June 21, 2020, from Federal Trade Commission: https://www.consumer.ftc.gov/blog/2019/07/equifax-data-breach-settlement-what-you-should-know

Radhakrishnan, S. (2015). COBIT Helps Organizations Meet Performance and Compliance Requirements. *COBIT Focus, 5*, 1-5. Retrieved from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=bth&AN=102026122&site=eds-live

Stevens, T. (2018). Global cybersecurity: new directions in theory and methods. *Politics and Governance, 6*(2), 1-4. doi:https://doi.org/10.17645/pag.v6i2.1569

Thomas, Z., & Adelwahed, S. (2017). Active Malware Countermeasure Approach for Mission Critical Systems. *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing*. doi:https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2017.11

Westcon-Comstor. (2018). *Security Lifecycle Review*. Retrieved June 21, 2020, from YouTube: https://youtu.be/agf1BdOHmMI

Weston, H., Conklin, T., & Drobnis, K. (2018). Assessing and resetting culture in enterprise risk management. *Assurances et Gestion Des Risques, 85*(1), 131-166. doi:https://doi-org.proxy1.ncu.edu/10.7202/1051319ar