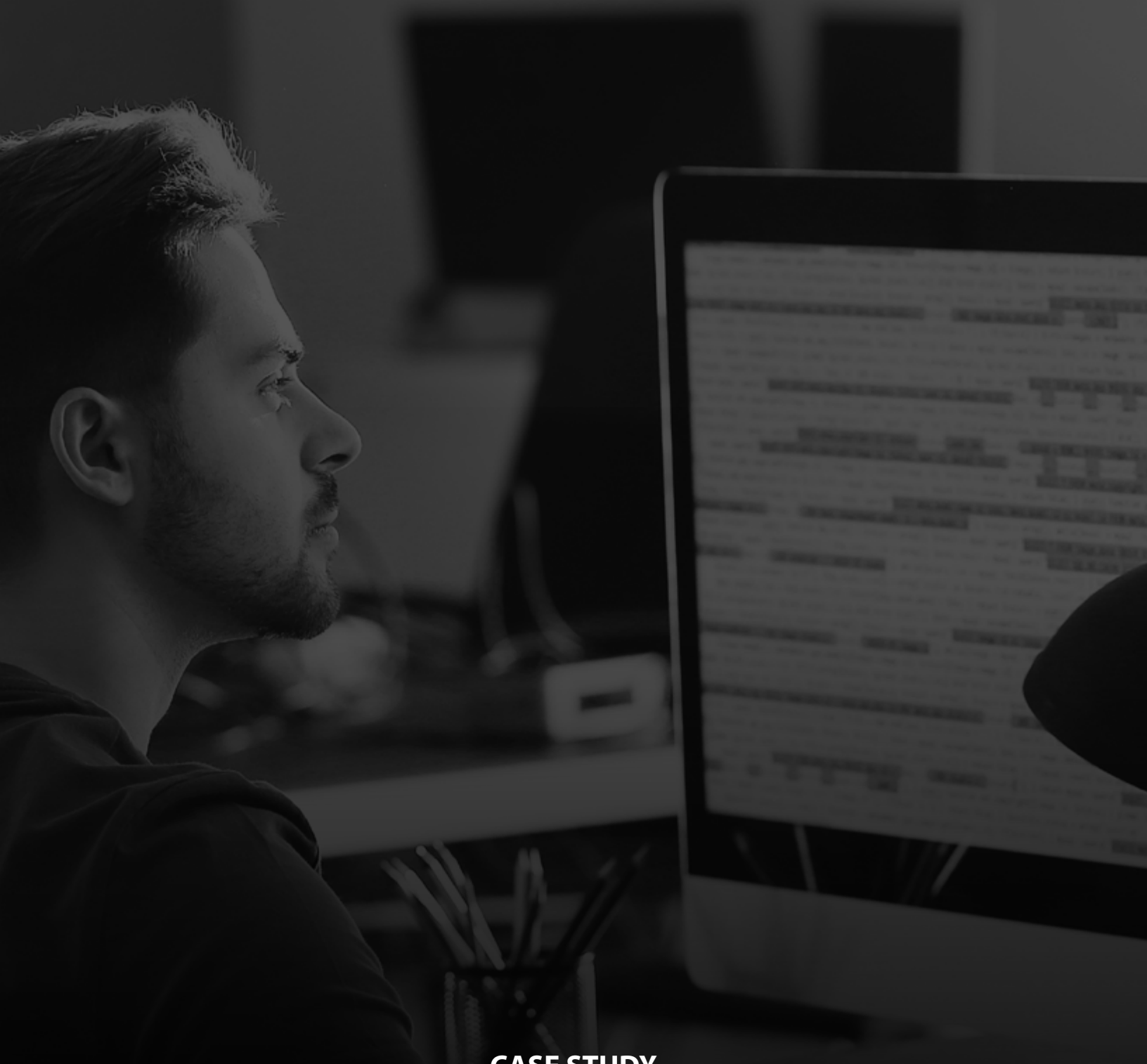


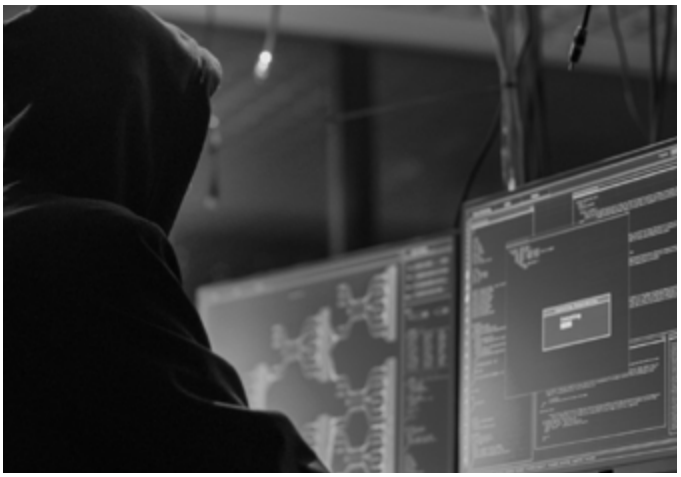
CASE STUDY

The Acme Inc. Incident

ACME Inc. is a global enterprise with several facilities spread across multiple countries and operating in several languages.

NERDS ON SITE®
TECHNOLOGY PARTNERS

The following describes the ransomware attack on an international company we will refer to as ACME Inc. (not the real company name) and the actions of the Nerds On Site Incident Response Team that thwarted the attack, mitigated the damage, got the company's critical systems back online with minimal downtime, and ensured those systems were properly fortified against further attack.

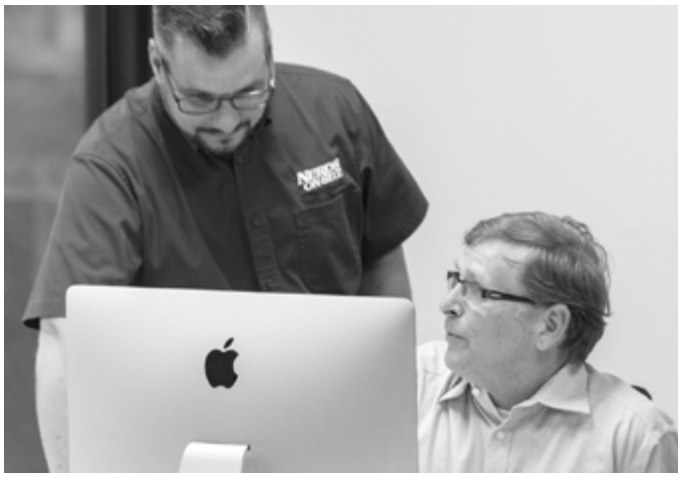


The Attack

January, 2019

The initial attack comes via email attachment (a phishing scheme) and launches a PowerShell script - a tool often exploited by cybercriminals as it falls under the radar of traditional endpoint security products. Over the next 6+ months, the Advanced Persistent Threat continues to infect systems across all of the company's global locations. At this point, the company is unaware of the specific threats as they go undetected by the McAfee Enterprise software ACME employs. 400 of the over 3000 internet-connected devices the company uses are infected.

By now, ACME's systems have become less and less stable due to the attackers' buggy software, which alerts the company to the threat.



Assessment & Investigation

July, 2019

Realizing they are under attack, ACME contacts Nerds On Site for support and the Incident Response Team responds immediately. The Team arrives and assesses the situation. Given the number of Indications of Compromise that are immediately visible, the Team is surprised that ransomware hasn't been deployed yet. In fact, it is in its final preparation stages. Isolation steps are taken and those "doors being closed" are noticed by the attackers who then launch the ransomware encryptor. The strike happens on the Friday evening at 6 pm—a favourite attack time as the attackers believe, with workers going home, this gives them the weekend to inflict maximum damage. However, the Incident Response Team remains vigilant and notices the encryption status shortly after it begins. The encryptor and ransom note (which demands a ransom of $600,000, increasing by $120,000 per day if not paid within a week) warn against shutdown and internet disconnection, but the Team does just that - shutting down every device in the data centre and the internet connection itself. This allows full preservation of at least one Active Directory domain controller that the encryptor had not yet compromised.

Response

The initial assessment and investigation of the incident gives the IR Team the best information it needs to initiate the Nerds On Site **3 Phase Incident Response Protocol**.

Phase One: Isolate

The Team removes the existing Cisco ASA gateways at site-to-site VPN infrastructure and replaces them with adam:ONE, the cutting-edge, DNS-based firewall and gateway solutions software. adam:ONE has a default "Holding Tank" policy. adam:ONE inserts a lifeline into the Holding Tank that gives infected devices limited internet access; only to Windows Update and Webroot - an advanced threat protection software —to ensure all security updates and patches are applied. With each endpoint automatically placed into Holding Tank policy, they have no access to an Active Directory and cannot do any further damage.

Phase Two: Remediate

The Team sets up every computer to boot into "safe mode" with networking support and deploys Webroot to do a thorough scan.

Locally, computers are brought into a large area where the Team works on 20 at a time. Across the other global locations, local IT teams under Nerds On Site direction, are given step-by-step instructions to do the same, translated into their language and communicated across a central dashboard that allows for a real-time view of global progress.

Once Webroot removes all known infections, the system is re-scanned in "normal mode" to ensure a clean status. Any and all Windows and applications updates are applied according to a "mission-critical", "important" and "can wait" priority.

Phase Three: Fortify & Maintain

Using adam:ONE technology, the Team reconfigures the systems starting from a Zero Trust standpoint using whitelisting. Whitelisting is the compilation of a list of all acceptable or known-safe applications - emails, IPs, devices, etc. - that you are going to allow to run on your systems and networks. Instead of the traditional blacklisting approach where any site or application not on a list of known bad actors is granted access to a site, whitelisting starts by allowing no-one access to the site. Then, once scanned and determined to pose no threat, all legitimately required internet resources and domains are added to the whitelist and made accessible to users. Any ongoing requests are managed with an adaptive whitelist approach that is supplemented with Artificial Intelligence.

The Results

Fast action on the part of the Nerds On Site Incident Response Team stopped the attackers in their tracks. Systems were brought back online with minimal damage, only one shift of downtime and without paying the ransom demanded. As importantly, the IR Team deployed technologies to ensure ACME Inc. is properly secured against future attacks.

Is Your Business Ready to Defend Itself Against a Cyber Attack?

CONTACT US TODAY TO BOOK A FREE ASSEMENT!

NERDS ON SITE®
TECHNOLOGY PARTNERS