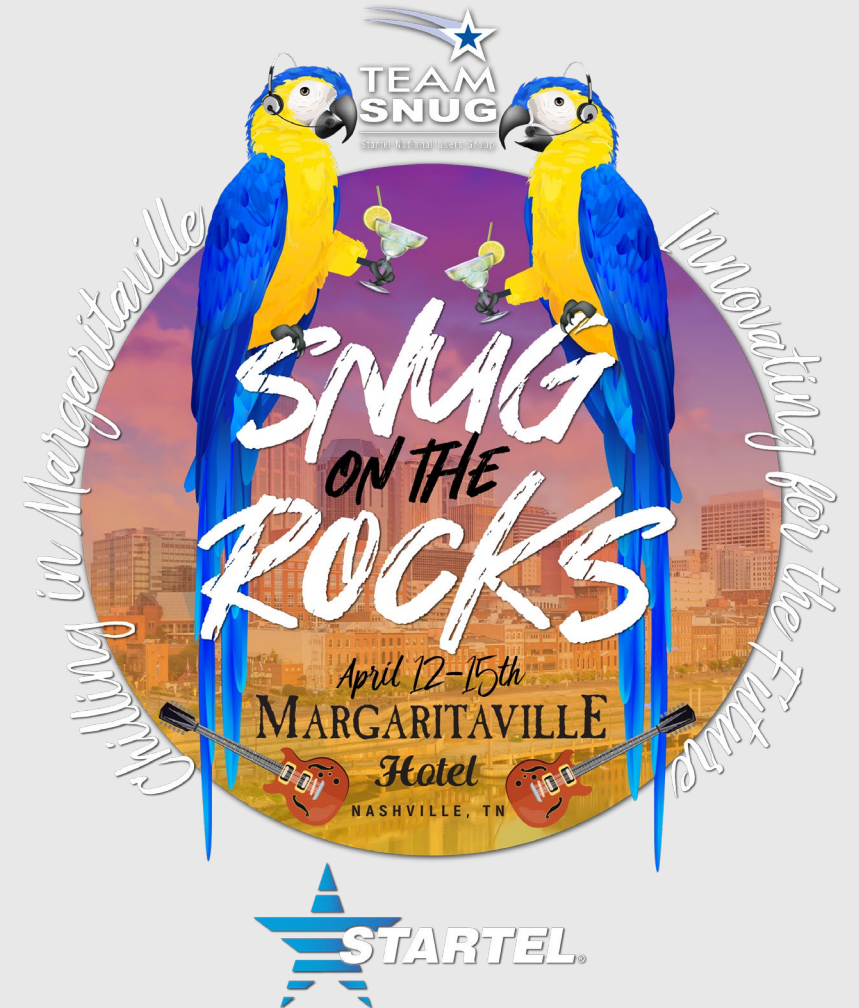


BPE RANSOMWARE ATTACK

Presented By Ray Shaw, BPE

September 9, 2018

Ransomware Attack and Recovery Steps



Cyber Attacks

It's not a question if it will happen –

It's when it will happen and what do you do when it does ??



We Are Under Cyber Attack !!

- On Sunday September 9, 2018, at approximately 6:15pm , while out to dinner with friends I received a call from my brother Michael (who was our On Call Manager), that we were under attack by Ransomware and that he had begun taking the preliminary actions required for our recovery until I returned home to assist
- Over the next several minutes, I will summarize what actions BPE took and by having a plan of action in advance – allowed us to take corrective steps to minimize our “downtime” and restore BPE to full Operations.



Chain of Events as confirmed by Forensics

- On Thursday 9/5/18 at 5:18am, BPE received an email from a BPE client with an attachment named “Request.doc”
- This email was later opened at approximately 11:34 AM from system SCJ-XD. The attachment itself was identified as a downloader Trojan and contained a macro which enabled a backdoor on the system which provided the attack a method to access the system directly.
- This attack was successful because the system had an unsupported version of Microsoft Office, due to another Program BPE was using, had not been updated to the current release



Trojan - Elevation of Privileges

- Once the initial foothold on the network was established by the attacker, credentials for Domain Administrator were obtained.
- The Domain Administrator account had been logged into this system previously and it is possible that a memory scrapping tool like Mimikatz was leveraged to obtain these credentials.



Lateral Movement & System Persistence

- On the days between September 5th and 9th, Forensics identified numerous forensic artifacts and Windows event log entries indicating the unauthorized access of systems by the adversary. The primary vector for access centered around Remote Desktop (RDP) and Secure Shell (SSH). The forensic artifacts surrounding the access activity suggest that the attacker was deepening their foothold on the environment (credential capturing software, network connections to command-and-control systems, scheduled tasks for data destruction, system configuration changes, and ransomware launcher toolsets).



Additional Forensic Analysis

- Although SCJ-XD was the initial foothold into BPE's network, based on the analysis, it appeared that the BPE-Domian Controller was leveraged as 'home base' for primary access to other servers across the network.
- This is especially concerning given the amount of access and control the bad actor would have at their disposal to remain persistent and successful with their objectives while on BPE's systems and network.



Deployment and Execution of Ransomware

- The deployment and execution of ransomware was done through the use of PowerShell.
- The actor was able to execute a scheduled task across various servers that leveraged PowerShell to execute a Base64 encoded string.
- These servers included: Glacier File Server, BPE-Domain Controller, and Logger1. When decoded, the string references the execution of a PHP script on a server located within the Netherlands over port 443.



Await Payment Message Appears

- After the attack had been launched, the attacker waits for the victim to contact them via email at “protonmail.com” and provides a public key to be disclosed in the email request to decrypt the files.
- These details are included in the ransom notes spread across the victim’s systems and network.
- The ransom notes file names were appended with ‘readme_txt’ and the encrypted files had the extension of ‘.locked’ appended



Re: File

to get the files in your network decrypted you should pay for the decryption software

the ransom amount is 120,000\$(one hundred twenty thousand US dollars) worth of bitcoins

we will provide bitcoin address when you ready

after we have the payment you will get the decryption software including instructions on how to use the decryptor



BPE To Pay or Not To Pay – That Was The Question ??

- Obviously, under no circumstances would BPE pay any ransomware
 - No Guarantee That the Files would be undecrypted after payment
 - BPE was Not Going To Fall Victim to a Cyber Terror Attack
- We would never know who was targeting us – was it an intentional (most likely not) attack or just random -- given it came from a client email (throw it out there and see what sticks)



VMWare / Data Center Licenses

- Several Things to Note ...
 - BPE utilizes Broadcom VMware vSphere (now VMWare Cloud Foundation)
 - BPE Utilizes Windows Data Server licenses (currently Windows Server 25 on its hosts
 - Ability to build and operate Windows 25 Servers and Terminal Servers “legally” .. Only require RDP & Client access licenses for the work stations that will connect



BPE Recovery Path Started

- Michael immediately contacted our IT Consultant, who recommended disconnecting all machines from the Internet and we then established a conference call and were able to connect to our data center from our Personal computers
- After the machines were disconnected from the Internet, each of the virtual machines was able to be isolated and analyzed – could they be recovered or restarted safely ???
- After reviewing our “Key Machines” – we immediately determined we needed to rebuild our network from Base “0” and at that point we were not sure client data recovery was possible



Concurrent BPE Staff Actions

- Our Customer Service Team and Shift Supervisors began notifying our clients that our service was down and unable to answer calls with no E-T-A of when our services would be restored
 - These notifications were done via an email list (hosted on GMail), faxes being sent thru our Ring Central account and telephone calls being made to our clients on the notifications list
 - Our Freeswitch (Session Border Controller) and Startel S3 Switch were not affected by the ransomware attack being Linux Boxes and once we confirmed they were safe to reconnect to the Internet and our VOIP providers, we initiated a “generic” announcement, informing callers of our inability to answer calls and in the event of an emergency to call 9-1-1



BPE Rebuild In Progress

- Affected Machines were isolated and preserved for future forensic analysis (7-year Statute Of Limitations)
- Rebuilding of Entire BPE Network infrastructure – most critical machines first
 - Domain Controller and reestablishment of users and their credentials
 - Revision of Permissions
 - Glacier (File Server) -Advantage Data Base Server
 - Application Servers
 - Terminal Servers
 - Voice Mail System Rebuild /required rerecording of greetings
 - Voice Logger (PTD)



There Was Some Good With The Bad That Happened

- Our application server had “survived” the attack – being disconnected from the network before the attack completed its execution, allowed us to scan the machine for trojans & viruses.
- Once Scanned, It was determined that we could recover our Client Data from the daily “Pinnacle Back-Up” which is stored on this machine, before being uploaded to our DR environment, which was also affected by the attack
- This Back-Up was extracted and scanned by Startel / PTD before being uploaded to our new Glacier File Server



Post Attack BPE Management Activities

- Notify BPE Insurers (Commercial Liability and Errors and Omissions) carriers and open “potential claims”
- Notify BPE Corporate Attorney of the Chain Of Events
- Attempt Contact With FBI (sat on hold for hours)
- Engage Cyber Forensics Specialist
- Determine if there was a HIPAA Data Breach ?
 - 60 Day Notification Period Started
- “Confidential” One on One Meetings with IT Departments of our healthcare clients to discuss the Chain Of Events and corrective actions being taken



PHI - Forensic Findings – HIPAA Breach ??

- However, as it relates to Personal Health Information (PHI) that was stored on BPE systems, this is a far more complicated assessment of risk.
- With that said, given the lack of forensic artifacts suggesting access of folders and files and evaluating cyber industry threat intelligence research (CrowdStrike) of the techniques, tools, and identified motives of the adversary, we view the potential risk to PHI on BPE's systems to be low.



Additional Post Cyber Attack Actions

- Rebuild Client TBS Billing
 - BPE had Paper Copies of Key Reports from our last billing from 8/21/18
 - TBS had a recent data back up
 - Requested Last 3 months Invoices from each BPE Client
- Recover Accounting / Management Files From Intuit Back Ups
 - BPE Quick Books Accounting
 - BPE Business TurboTax – Tax Filing Copies
 - Microsoft Documents (Word, Excel), PDF Documents
- Implemented Security Information and Event Management (SIEM)
- Implemented Crowd Strike in place of Sophs Anti-Virus
- Implemented Regular Penetration & Vulnerability Scans



Office Of Civil Rights Audit

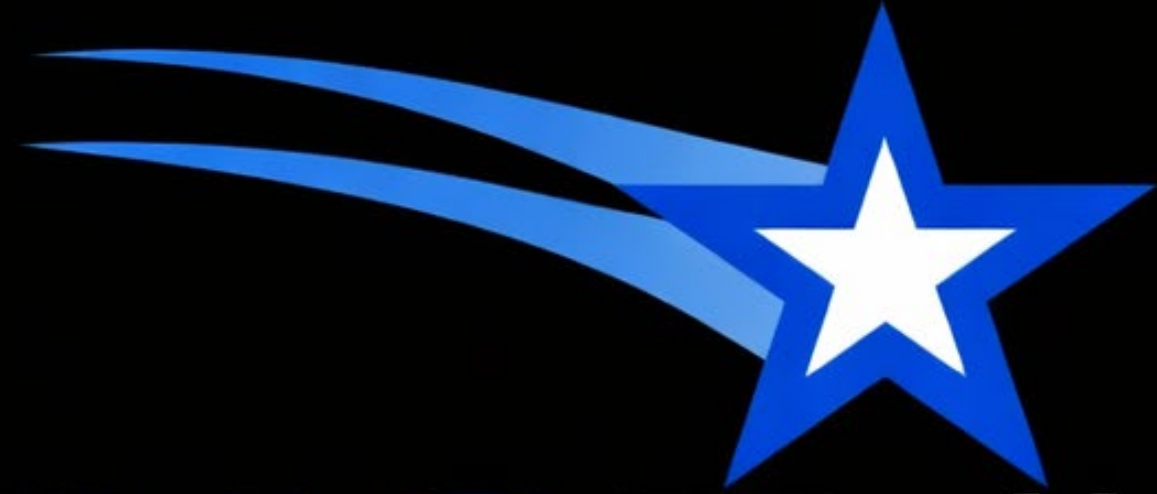
- Based on Our Cyber Forensic Findings, one of Health Care clients filed an unnecessary breach notification with the Department Of Health and Human Services Office For Civil Rights which set off another chain of events
- After undergoing a months long strenuous “paper” audit – we were found clear of any wrongdoing in the cyber incident
 - Having Clear Policies and Procedures in Place which were followed
 - Able to Provide copies of client notifications
 - Forensic Audit Results



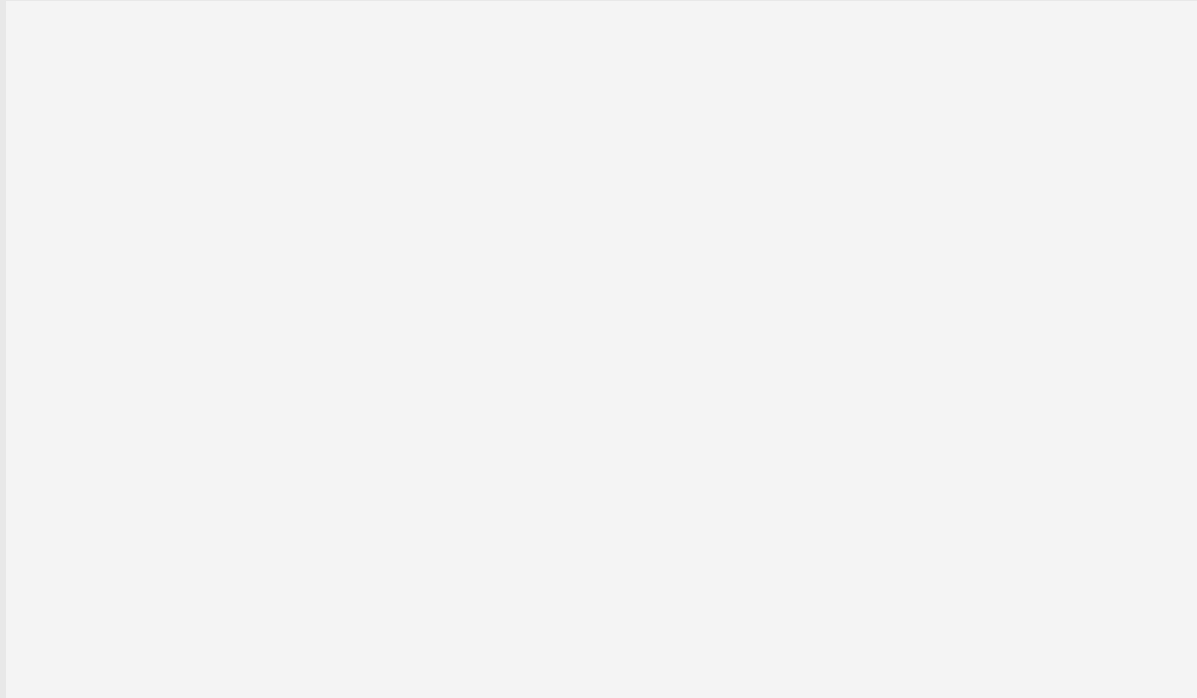
Current BPE Activities – Post Ransomware Attack

- Working With Van Rein Consulting to obtain a SOC2 Audit
- Have reached the 7-year statute of limitations
- Have successfully undergone several security audits by our healthcare clients
- Have updated Policies and Procedures to be followed
- Constantly updating our Business Continuity Plan
- Keeping Our Data Center Equipment and Software Updated and Patched





SNUUGTalks



TEAM SNUG
Startel National Users Group

Chilling in Margaritaville

SNUG ON THE ROCKS

Innovating for the Future

April 12-15th
MARGARITAVILLE
Hotel
NASHVILLE, TN

STARTEL