NETWORK SECURITY CASE STUDY

By James Cassidy

Analysis of General Network Security Issues

Initial analysis of the Potayto Crisps network reveals major vulnerabilities in how the network is setup, as well as hardware and software utilised. Left in its current state, attackers will exploit these vulnerabilities and could potentially bankrupt the company.

Several issues have been identified, including:

- The factory site is comprised of five departments that all share the same network and single LAN. The lack of network segmentation poses a serious risk as an attacker will have access to all hosts on the network should they chose to attack.

- A Juniper Networks SR110 device provides access to the entire site. Further inspection into this device reveals a 'traffic classification vulnerability exists, allowing an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorised resources'[1] within the factory's network. This affects the device used by the factory and as no changes have been made to it in six years, it still exists. With a CVSS score of 9.8 (critical), it's imperative that this exploit is patched immediately.

- The gateway router used is a TP-Link TL-SF1048 Unmanaged switch. This has a number of security risks associated with it including open ports and no network monitoring. Ports cannot be disabled on an unmanaged switch, easily allowing unauthorised accessed by an attacker. Protocols such as SNMP don't exist on unmanaged switches that can determine the health of the entire network. Therefore, the company may be unaware an attack has ever taken place. The addition of Wi-Fi on the switch allows unauthorised devices to connect or expose communications to sniffing and replay attacks.

- A NAS from vendor QNAP is utilised by the company. QNAP recently reported that 'ransomware and brute-force attacks have been targeting their networking devices. They recommend disabling port forwarding of NAS management service port 8080 and 443 on the gateway router and disabling the UPnP function of the QNAP NAS'[2]. Ransomware will encrypt the company's 'Onion & Cheese' flavour and demand ransom in exchange for encryption. It is imperative this issue is resolved immediately to ensure confidentiality of Potayto Crisp flavours remain intact.

- The research department utilises Windows Server 2012 R2. Within this exists a vulnerability that allows 'unauthenticated remote code execution. This is done by an attacker connecting to the target system and using the Remote Desktop Protocol to send specially crafted packets and requires no user interaction. From here, they can then install, change, or delete data as well as create new accounts with administrative rights.'[3] This is a critical issue with a CVSS score of 9.8. Should an attacker exploit his vulnerability they will have complete control of the research department and eventually the entire company network. It is imperative this is tackled immediately.

[1] 'CVE-2022-22167', https://www.opencve.io/cve/CVE-2022-22167

[2] 'Take Immediate Action to Secure QNAP NAS', https://www.qnap.com/en/security-news/2022/take-immediate-actions-to-secure-qnap-nas

[3] 'CVE-2020-0609', https://vulmon.com/vulnerabilitydetails?qid=CVE-2020-0609&scoretype=cvssv3

- General administrative office uses Siemens SICAM Toolbox II software to oversee onsite renewable energy generation. Within this software exists a 'vulnerability with a CVSS score of 9.9 (Critical) that can be exploited remotely. It allows a successful attacker access to the company's database'[4]. As this software is being used by the general administrative office, an attacker will gain access to all employee and company records etc.

Analysis of the threat posed by 'Conti Ransomware'

Conti ransomware is a malicious program that works by preventing a user from accessing their data (via encryption) unless a ransom is paid. Conti ransomware will then spread laterally within the network via the SMB port (445) and encrypt files on different hosts. This could potentially compromise an entire network.

Conti threat actors often gain initial access through phishing attacks or weak RDP credentials to install TrickBot and BazarLoader trojans that subsequently provide remote access to the infected hosts. The ransomware then begins to move laterally through the network, stealing credentials and harvesting unencrypted data stored within the network. These attackers are known to exploit remote management and management software to maintain a persistent backdoor within the network.

'Artifacts leaked from their playbook identify four IP addresses Conti actors previously used to communicate with their command-and-control server.'[5]

- 162.244.80.235
- 85.93.88.165
- 185.141.63.120
- 82.118.21.1

In the case of the Potayto Crips network, various indicators of compromise exist that make it susceptible to this Conti Ransomware attack.

Through the wireless access point located on the switch, Conti actors can perform a man-in-the-middle (MITM) attack by abusing ARP using a tool such as 'ettercap'. AN ARP reply is sent to the router that sends traffic to the attacker's MAC address rather than the intended host's IP address. This can include credentials such as login details for Windows Server 2012 R2.

From here, they can begin to attack internet-facing remote desktop protocol that exists within Windows Server 2012 R2. Sending specially crafted packets, Conti actors can begin to install trojans such as BazarLoader and TrickBot, as well as create a new administrative account, escalating attacker privileges.

Deep Packet Inspection rules are bypassed, allowing the malware to be installed without getting being detected due to the vulnerability that exists within the Juniper SRX110 device. Furthermore, lack of protocols such as SMNP on an unmanaged switch, the company would be unable to determine the health of the entire network and determine whether malware had been installed or not.

[4] 'ICS Advisory (ICSA-22-041-05)', https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-05

[5] 'Alert (AA21-265A)', https://www.cisa.gov/uscert/ncas/alerts/aa21-265a

Conti Ransomware will attempt to move laterally within the network. As no network segmentation or segregation has been established within the factory site, the threat actors now have essentially full control of the departments and data contained within.

Through the Siemens SICAM Toolbox II software vulnerability, Conti threat actors will exploit this and encrypt all contents of Potayto Crisps database, including employee details, and company finances.

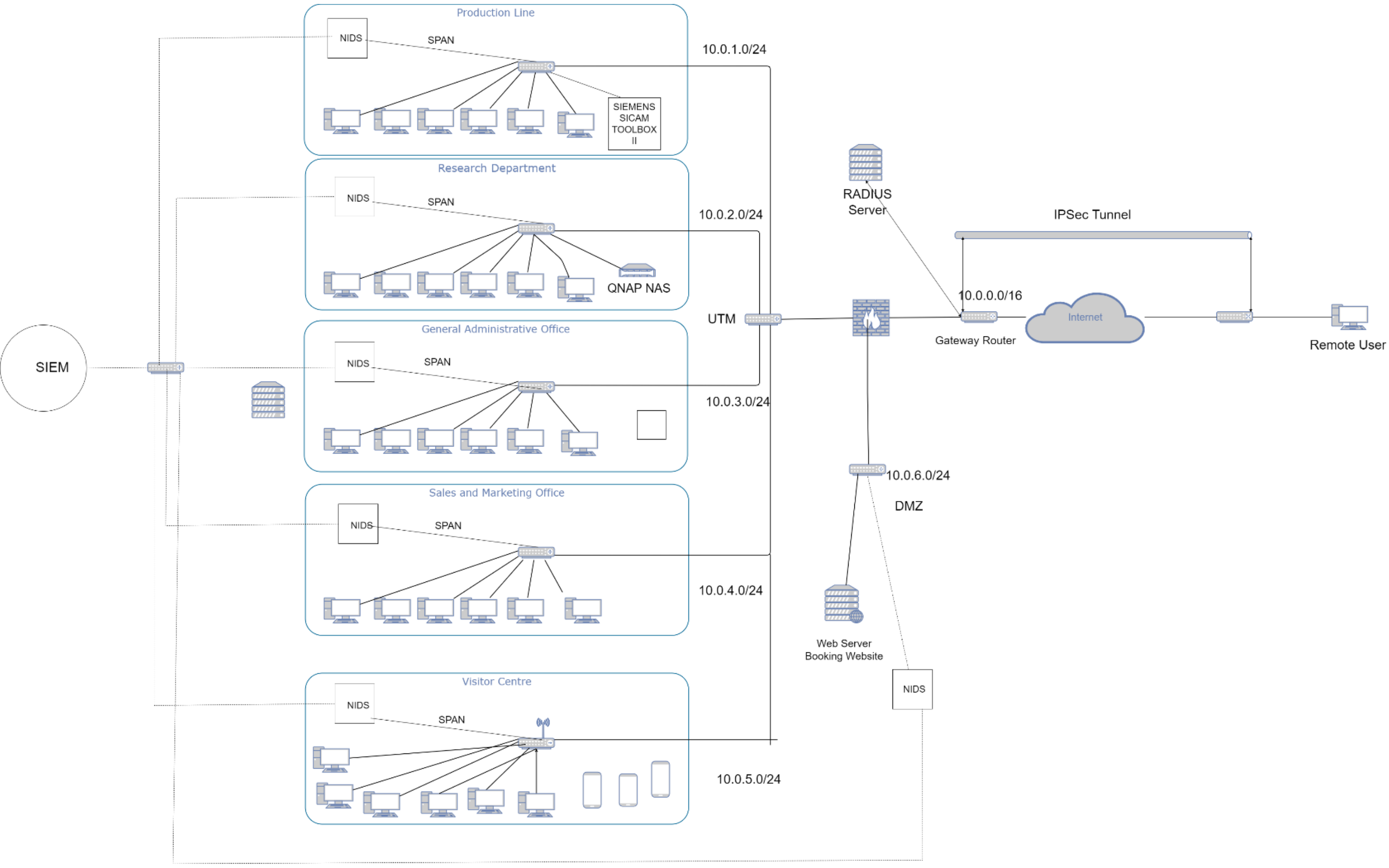
As a backdoor is maintained through Siemens SICAM Toolbox II, threat actors could potentially shutdown the renewable energy generation, causing disruption to the production line should Potayto Crisps chose not to pay the ransom, costing millions.

With all ports on the network being open through the unmanaged switch and with port forwarding enabled on the QNAP NAS, it is almost certain all data within the NAS, including all unique and valuable recipes, will be encrypted by Conti ransomware.

Network Security Recommendations

Based on the information gathered from initial analysis of the Potayto Crisps network, several improvements have been made to both detecting and protecting the factory network from malicious threat actors, including Conti Ransomware.

These improvements can be found in the network diagram below:



Originally the entire factory site was comprised of a single LAN. To combat this, network segmentation has been implemented comprising of 5 different VLANs connected to a new TP Link TL-SG3452 Managed Switch. SNMP protocol is supported on this switch allowing for management and monitoring of all network devices on the network.

This architectural approach divided the network into multiple subnets, each acting as their own small network. In the diagram, five subnets have been created. Each subnet now has an IP address range of 256, instead of entire network having access to 16,777,216 addresses. Robust network segmentation between each subnet reduces the spread of Conti Ransomware by preventing lateral movement of the malware, trapping it in that network segment.

The visitor centre subnet utilises Wireless Access Point, allowing employees to connect to the network wirelessly. A captive portal has been setup, requesting users to authenticate themselves before being allowed on the network.

Each subnet is connected to one Unified Threat Management (UTM), and acts as a firewall for all 5 subnets. This firewall can be configured to block TCP port 445 (SMB) to prevent Conti ransomware from disturbing itself throughout the network, as well as blocking domain names and IP addresses associated with Conti Ransomware.

Each subnet has very different business operations associated with them resulting in different security risks, threats, and functions. This requires the development and enforcement of separate network security policies. For these network policies, Network Intrusion Detection Systems (NIDS), each with different security policies. For example, stricter rules may be applied to the research department as it is seen as a critical subnet with the creation of various new flavours, while General Administrative Office centre may see more common SNORT rules applied to it.

Each NIDS is connected to the switch of each subnet through the SPAN port which is then fed back to a Security Information and Event Management (SIEM). The SPAN port takes a mirrored copy of network traffic, which is then sent to the SIEM to aggregate, store, and display this data. Logging is key for incident response should a Conti Ransomware attack occur.

A DMZ (Demilitarized Zone) has been established, containing internet-facing services including the web server containing the booking website as well as remote access for the supplier of the specialised analysis equipment. Should a Conti actor exploit the Remote Desktop Protocol vulnerability that exists within Windows Server 2012 R2, the DMZ will be compromised. However, the UTM separates the VLANs from the DMZ, keeping the private network secure and making reconnaissance of the network impossible.

An IPSec VPN will now be utilised for clients that wish to access the network remotely. Previously, remote clients were connecting to the network via a public network such as the internet. This allows anyone, including Conti actors, to eavesdrop, sniff packets and potentially spoof IP addresses.

IPSec establishes security at the network layer and offers a suite of protocols including Authentication Headers, Encapsulating Security Payloads and Security Associations. Tunnel Mode utilises all these protocols to ensure IP packets remain secure between the remote client and private network.

Access Control with IEEE 802.1x has also be implemented into the network. Should a Conti actor try to gain access, the gateway switch will act as an authenticator and block ingress traffic from the supplicant. The switch works in conjunction with a RADIUS Server, providing multi-factor authentication. The credentials are passed to the RADIUS server for verification, making it significantly harder for a Conti actor to gain unauthorised access and ensures only genuine remote clients gain access to the network.

To ensure valuable crisp flavours remain private, NAT port forwarding has been disabled on the QNAP NAS. This will prevent genuine external suppliers from accessing the recipe as HTTPS port 443 will be disabled alongside port 8080. This is the only trade off with the implementation of this network. However, it will be more difficult for Conti Ransomware to find and encrypt all data on the NAS.

Finally, software updates have been made to the Juniper Networks SRX110 device to ensure Deep Packet Inspection is not bypassed. This form of packet filtering will block specific data or code payloads. Trojans utilised by Conti actors including BazarLoader and Trickbot will therefore be blocked by DPI.