Company XYZ

Report of Cyber Incident

Date of Compromise: May 4, 2020

Number of Systems Impacted: 20

Type of System Impacted: Windows Workstations (15), Windows Servers (5)

Description:

On May 4, 2020, the cyber operations unit found evidence of an intrusion to the computational infrastructure.

The first indication of the intrusion was an NIDS alert which showed network traffic leaving 3 of the Windows user workstations on port 4444. The team investigated the incident further to reveal that the traffic originated from a program with the SHA256 hash of FF79D3C4A0B7EB191783C323AB8363EBD1FD10BE58D8BCC96B07067743CA81D5. Host based firewalls were adjusted to allow this traffic to flow.

To maintain persistent access to their targets, the attackers employed tactics involving scheduled tasks, the Windows registry and Windows Management Instrumentation. Registry keys and WMI subscriptions were included in common autorun locations for these Windows components.

Additional actions taken by the adversaries were bypassing the Powershell Script Execution Policy, thus violating standard IT practices.