Ashley Furr raised this on 22/Aug/23 5:06 PM

Description

Description:

On August 21st, between 2:21 pm and 3:31 pm, Stellar Cyber observed multiple Internal Trojan alerts. These alerts were raised as a result of a possible malware trojan disguising as legitimate software to gain access to an internal system or files. The domains associated with the alerts are misspelled which suggests that the attackers are URL hijacking and posing as other platforms.

Stellar Incident Link

Recommendations and Questions:

We recommend blacklisting the domain names associated with the alerts, run antivirus scans on the hosts, and encourage users to be aware of phishing emails as GameOver Zeus is often propagated through spams and phishing messages.

Question:

Do you recognize any of these IP's or domains that are trying to access your AD servers?

Additional information:

GameOver Zeus P2P Malware

GameOver Zeus Switches from P2P to DG

Alert 1: Internal Trojan, August 21st, 2:21 pm

- Network IDS in internal traffic discovered a malware trojan (malware disguised as legitimate software in order to gain access to a system or files) between "[redacted] and "[redacted] matching IDS signature "TROJAN Possible Zeus GameOver/FluBot Related DGA NXDOMAIN Responses" with IDS severity "critical".

- **Source Host**: [redacted]
- **Destination Host:** [redacted]

Alert 2: Internal Trojan, August 21st, 3:19 pm

Network IDS in internal traffic discovered a malware trojan (malware disguised as legitimate software in order to gain access to a system or files) between "[redacted]" ([redacted]) and "[redacted]" ([redacted]) matching IDS signature "TROJAN Possible Zeus GameOver/FluBot Related DGA NXDOMAIN Responses" with IDS severity "critical".

- **Source Host**: [redacted]
- **Destination Host**: [redacted]
- **Domain Name Associated with Alert**: [redacted]

Alert 3: Internal Trojan, August 21st, 3:19 pm

- Network IDS in internal traffic discovered a malware trojan (malware disguised as legitimate software in order to gain access to a system or files) between "[redacted]" ([redacted]) and "[redacted]" ([redacted]) matching IDS signature "TROJAN Possible Zeus GameOver/FluBot Related DGA NXDOMAIN Responses" with IDS severity "critical".

- **Source Host**: [redacted]
- **Destination Host**: [redacted]
- **Domain Name Associated with Alert**: [redacted]

Alert 4: Internal Trojan, August 21st, 3:31 pm

- Network IDS in internal traffic discovered a malware trojan (malware disguised as legitimate software in order to gain access to a system or files) between "[redacted]" ([redacted]) and "[redacted]" ([redacted]) matching IDS signature "TROJAN Possible Zeus GameOver/FluBot Related DGA NXDOMAIN Responses" with IDS severity "critical". Destination Host: [redacted]

- **Source Host**: [redacted]
- **Destination Host**: [redacted]