Jun 21 2023

NETMANAGEIT

Intelligence Report

Analysis of Ransomware With BAT File Extension Attacking MS-SQL Servers (Mallox)

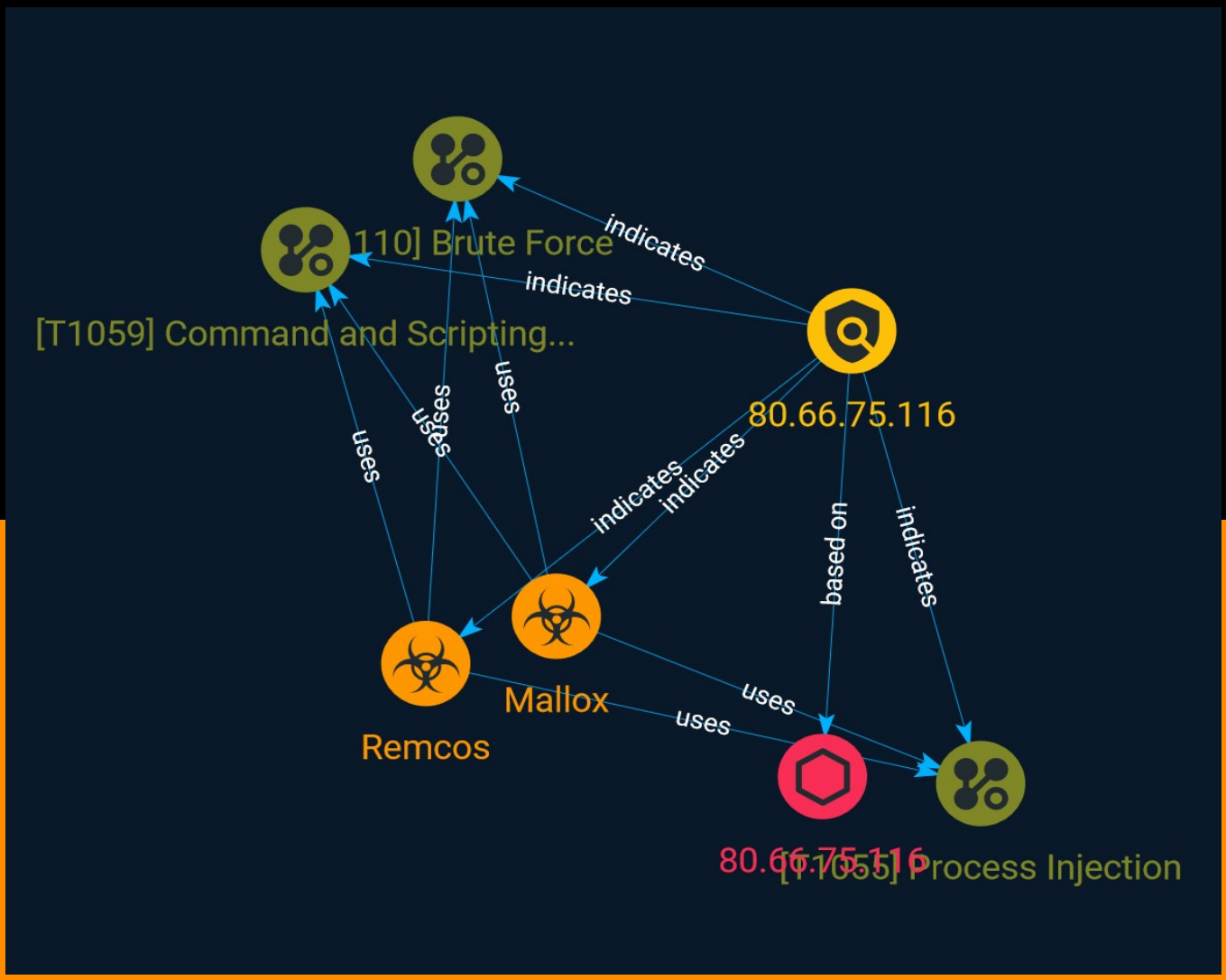

Table of contents

Overview

Entities

Observables

External References

Overview

Description

AhnLab Security Emergency response Center (ASEC) has recently discovered the Mallox ransomware with the BAT file extension being distributed to poorly managed MS-SQL servers.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Attack-Pattern

Name
Brute Force
ID
T1110
Description
Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes. Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy Discovery](https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access.
Name
Process Injection

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries

may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Indicator

Name

80.66.75.116

Description

ISP: Kakharov Orinbassar Maratuly **OS:** Windows Server 2012 R2 (build 6.3.9600) ---------- Hostnames: ---------- Domains: ---------- Services: **445:** ``` SMB Status: Authentication: enabled SMB Version: 1 OS: Windows Server 2012 R2 Standard 9600 Software: Windows Server 2012 R2 Standard 6.3 Capabilities: extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks, lock-and-read, lwio, nt-find, nt-smb, nt-status, rpc-remote-api, unicode ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Tue, 20 Jun 2023 17:14:35 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: WIN-CLJ1B0GQ6JP NetBIOS Domain Name: WIN-CLJ1B0GQ6JP NetBIOS Computer Name: WIN-CLJ1B0GQ6JP DNS Domain Name: WIN-CLJ1B0GQ6JP FQDN: WIN-CLJ1B0GQ6JP ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '80.66.75.116']

Malware

Name
Mallox

Name
Remcos

IPv4-Addr

Value
80.66.75.116

External References

- https://asec.ahnlab.com/en/54704/
- https://otx.alienvault.com/pulse/64930715aacf3f3a02115e11