Threat Emulation Assessment Report: APT 10

Developed by: Cyber Protection Team 169

CW3 James Honeycutt

Threat Emulation Assessment Report

# Executive Summary

*Cyber Protection Team (CTP) conducted a threat emulation operation on 18 March 2021. The CPT emulated threat actor APT10, a.k.a menuPass. APT10 has been known to hide in plain sight using common tools built into the system to steal secrets. The operation worked under the assumption of assumed breach, meaning the breach was simulated and no breach occurred. Once the CPT was on a machine, they were able to retrieve a list of local administrators and steal some passwords. They also established persistence by creating a scheduled task. From the local workstation they were able to enumerate all the computers in the domain and get a list of running processes from the domain controller. Using a common administrator tool, they were able to laterally move to the domain controller. Once on the domain controller, they stole more passwords.*

## Scope

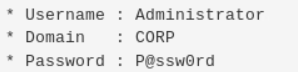
*The scope of the operation was to use common tools built into the operating systems and open-source tools to enumerate the network and obtain proprietary documents.*

## Key Findings and Recommendations

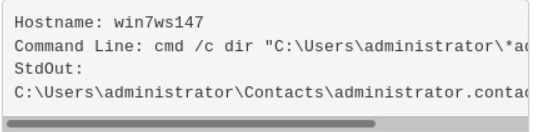
*The CPT was able to obtain some administrator credential and succeeded at enumerating the domain. Then account was using a weak password and recommend forcing the use of password complexity and dual factor authentication for administrators. They were able to locate some administrator documents in a non-secure location. Recommend keeping sensitive documents in a secure file server or data storage.*

# Assessment Findings

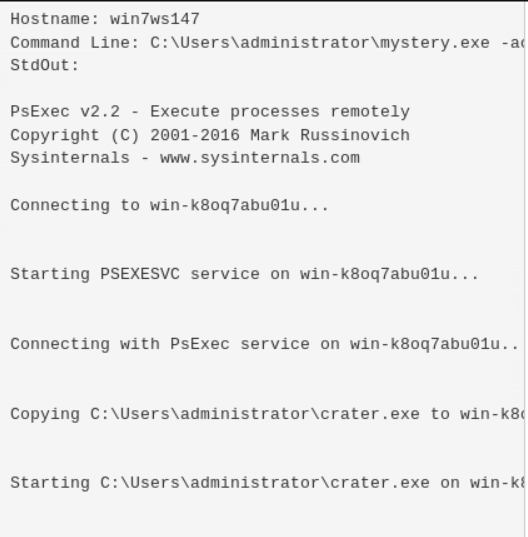
*Using MimiKatz the CPT was able to get the local administrator credentials of Win7ws147. Command used ‘ sekurlsa::logonPasswords’*

**

*The same machine also had the sensitive document. Command ran `cmd /c dir “c:\users\administrator\\*admin\*” /b /s /a-d’ The command found “c:\users\administrator\Contacts\administrator.contact”*

**

*The CPT was also able laterally move to the domain controller using PSEXEC. PSexec was renamed to mystery.exe. The command used “c:\Users\administrator\myster.exe -acceptelua -u corp\administrator -p P@ssw0rd -d -cv c:\users\administrator\crater.exe* [*\\win-k8oq7abu01u*](file:///\\win-k8oq7abu01u)

**

# Conclusion

*The over all issue is with the administrator accounts. Most of everything that the CPT accomplished could have been avoided by protecting the domain administrator account. One recommendation is to not let anyone use the builtin domain administror account and create an extremally long password for it. The admins who work as domain admins should have two account. One account to log into machines and a privileged account to perform administror functions. The privileged account should be set up as dual factor, this way it will take more than an off the shelf tool to steal the credentials to your environment.*

# Appendix

*Here is where I would attach my TEA’s.*

*I would also attach the BSF from Caldera along with more screen shots.*

*Any custom scripts that I created for this operation would be attached.*

*Any other documentation that I thought would help the defenders would also go here.*