Raytheon
Blackbird Technologies

20150821-261-CERT-EU
Kerberos Golden Ticket

For

SIRIUS Task Order PIQUE

Submitted to:

U.S. Government

Submitted by:

Raytheon Blackbird Technologies, Inc.
13900 Lincoln Park Drive
Suite 400
Herndon, VA 20171

21 August 2015

(U) Table of Contents

1.0 (U) Analysis Summary

(S//NF) This report covers two reports on an attack known as "passing the golden ticket", a Kerberos TGT ticket. One report was provided by CERT-EU titled, "Protection from Kerberos Golden Ticket", and the other report a slide deck from the 2015 RSA Conference titled, "Hacking Exposed: Beyond Malware." The RSA Conference slide deck touches on passing the golden ticket. The CERT-EU report focuses, as the title suggests, on detecting and mitigating a passing the golden ticket attack and there are essentially no technical details on how to perform the attack. The RSA Conference slides provides some redacted PowerShell script commands that invoke mimikatz to build a golden ticket, but little technical discussion on implanting an attack from beginning to end. The report describes what access and artifacts are required to build a golden ticket, but it does not provide any technical details in achieving the required level of access or pivoting to collect the necessary artifacts.

(S//NF) The pass-the-ticket attack is similar to pass-the-hash attack except that a Kerberos ticket is passed instead of an NTLM/LanMan hash. As with the case with pass-the-hash attacks, the pass-the-ticket attack is a two-step process:

1. Capture the credential from memory of a compromised host, the Kerberos ticket (TGT or ST) in this case. This requires:
   a. Having control on a compromised host in the target network (via spear phishing, social engineering, etc.).
   b. Having high privilege or SeDebug privileges on the compromised host (privilege escalation tools can be used once a beachhead is established). Elevated privileges allow access to memory (i.e., LSASS) and enables credential harvesting from memory.
2. Replay the ticket to access resources:
   a. Once the credential is harvested, the attacker can use it to gain access to other resources such as another host or server (pivot). The mimikatz tool provides utilities to extract the Kerberos credentials from a target memory dump and craft a golden ticket from the credentials harvested.
   b. A Kerberos golden ticket representing a privileged user on the target can enable the attacker to copy the entire Active Directory from the target.

(S//NF) The preceding description of a pass-the-ticket attack is the level of detail provided by the report, i.e. no technical details on how to implement the attack from gaining access to leveraging the ticket, simply a high level overview of the pass-the-ticket attack taxonomy.

(S//NF) Although an interesting and well-written report, there are no technical details sufficient to warrant a PoC recommendation.

2.0 (U) Description of the Technique

(S//NF) Not applicable as no PoCs are recommended.

3.0 (U) Identification of Affected Applications

(U) Windows.

4.0 (U) Related Techniques

(S//NF) Privilege escalation, pass-the-hash, and memory forensics.

5.0 (U) Configurable Parameters

(S//NF) Varied depending on target.

6.0 (U) Exploitation Method and Vectors

(S//NF) No exploitation methods were discussed in this report. The only attack vector mentioned was spear phishing.

7.0 (U) Caveats

(U) None.

8.0 (U) Risks

(S//NF) Not applicable as no PoCs are recommended.

9.0 (U) Recommendations

(S//NF) No PoCs are recommended.