Assignment #5

CPEN 442

Ben Henaghan
Department of Electrical and Computer Engineering
University of British Columbia
Vancouver, Canada
Student Number: 96671466

Scott Wang
Department of Electrical and Computer Engineering
University of British Columbia
Vancouver, Canada
Student Number: 72573322

Austine Yapp
Department of Electrical and Computer Engineering
University of British Columbia
Vancouver, Canada
Student Number: 86705340

Mike Yue
Department of Electrical and Computer Engineering
University of British Columbia
Vancouver, Canada
Student Number: 24583156

I. PROBLEM #1

Selected malware: Dridex

A. Analyze the design of the picked malware, i.e., its structure, behavior, mechanisms it uses for selecting victims, infecting them, hiding itself and its authors, etc.

Dridex is a type of banking trojan that specializes in stealing bank credentials and other personal information through HTML injections. The malware mainly targets customers of major online banking/financial institutions based in Europe. The spread of Dridex utilizes social engineering by sending seemingly harmless Microsoft Office documents via email to unsuspecting victims. When a target opens the email attachment and allows the use of Microsoft Office macros, the macro downloads the main payload of the virus, the Dridex malware, which installs and runs on the victim's computer. Once installed on an infected system, an adversary may execute various actions such as:

- Upload files
- Download files
- Execute files
- Monitor network traffic
- Browser screenshot taking
- Add the compromised computer to a botnet
- Communicate with other peer nodes through the peer-to-peer (P2P) protocol to retrieve configuration details
- Download and execute additional modules
- Download and execute additional files
- Inject itself into browser processes for Internet Explorer, Chrome, and Firefox in order to monitor communications and steal information.

Dridex employs the following network infrastructure, as shown in Fig. 1.

In most instances, the victim's bank credentials are compromised through keystroke monitoring or taking a screenshot during an internet banking session. Although Dridex is most commonly associated with being a banking trojan used for stealing online banking credentials, it also has the ability to redirect HTTP traffic, steal cookies, steal form data, etc. This could potentially lead to further privacy violations of other online accounts such as social media.

Dridex has been constantly updated with new capabilities. In recent times, changes have been made to Dridex that aim to avoid detection by anti-virus systems. Anti-virus software mainly relies on incompatible file signatures (MD5 or SHA256 hashes) to detect malicious files. To avoid detection, Dridex leverages on newly created and signed 64-bit dynamic link libraries (DLLs), which have different file signatures from their earlier versions. These DLLs are sideloaded via legitimate Microsoft Windows binaries and appear to be part of a legitimate software product, making detection even more difficult.

Dridex malware is an evolution of the Cridex malware that is based on the ZeuS Trojan Horse malware, and is distributed by the Necurs botnet.

B. Identify the aspects specific to your malware that can be used to detect or prevent it

Firstly, Dridex malware is spread through malicious Microsoft Office documents. As such, only users of Windows computer may be affected; Dridex cannot install itself on other PC operating systems, such as macOS or Chrome OS, nor can it load on mobile operating systems, such as iOS and Android.

Furthermore, Dridex utilizes Microsoft Office macros to infect its victims. Users should thus disable macros in Microsoft Office and be careful of opening Word and Excel file attachments sent from unrecognized email addresses.

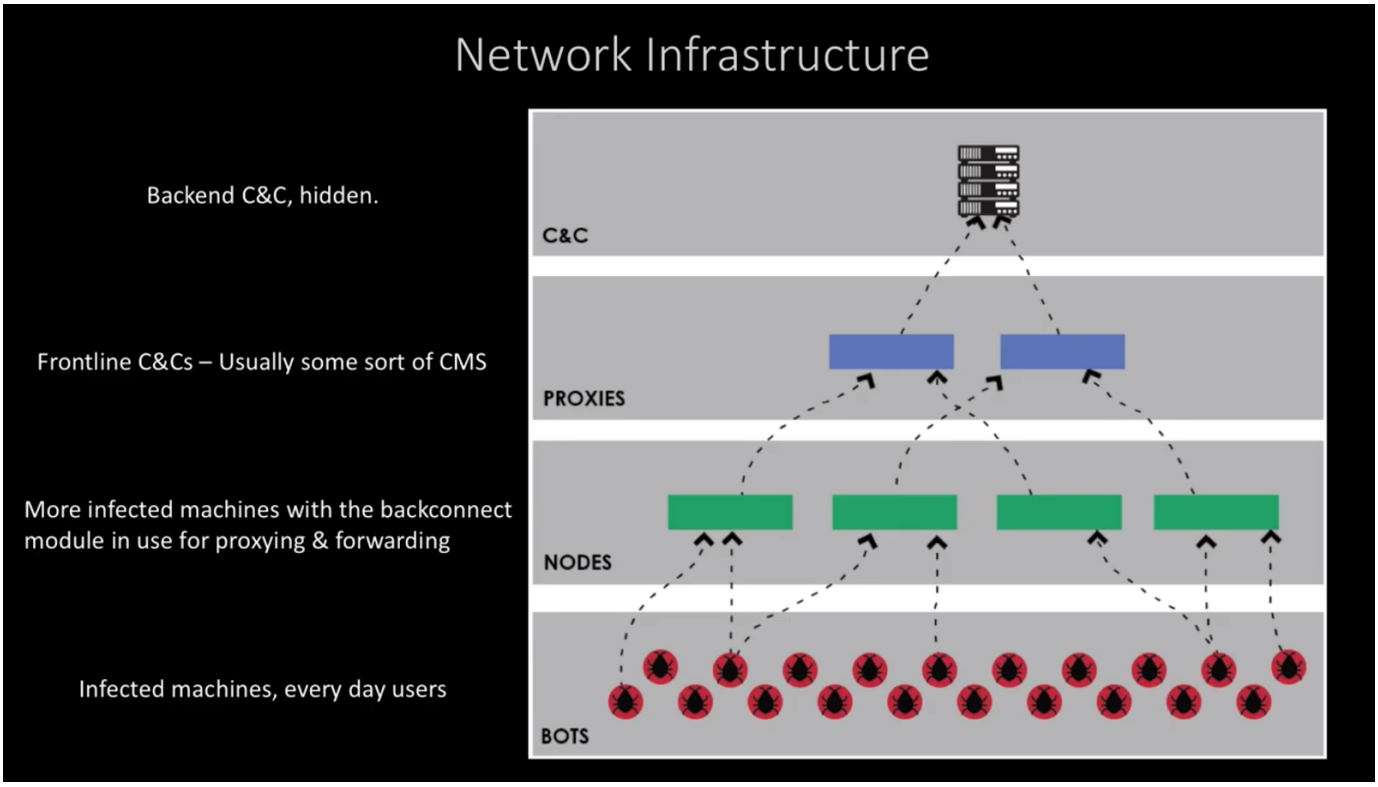

Fig. 1. Network infrastructure of Dridex

C. Based on your analysis, recommend short, medium and long term countermeasures (i.e., protection and detection techniques) against the threat posed by this malware.

Short term countermeasure: If DRIDEX infection is suspected or detected, immediately change the online banking account passwords using a different (and hopefully uninfected) system, and touch base with the bank to alert them for any fraudulent transactions taking place. Do the same for any account that you may have accessed using your infected system.

Medium term countermeasure: Delete any suspicious-looking emails you receive, especially if they sport links and/or attachments. Don't even open them, just delete them. If they purport to come from legitimate organizations, verify with the organization in question first.

Long term countermeasure: Install an antimalware solution that also covers email in its protective scope. This should remove the chance of you accidentally opening malicious email/malicious attachments in the first place.

II. PROBLEM #2

We wrote the solution steps of some lessons that we have solved it but the icon didn't turn to green.

A. General: Google Chrome Developer Tools

Lesson 4:

1) Used the console in the dev tools and call the javascript function webgoat.customjs.phoneHome()
2) Got the random number in console: 669788521

Lesson 6:

1) Used the network tool in the dev tools to capture the request
2) Found the network number: 36.45863852087676 in data section.

B. Injection Flaws: SQL Injection(advanced)

Lesson 3:

1) Used SQL injection:

$$Dave'; SELECT * FROM user\_system\_data; --\quad (1)$$

2) We can find the password of Dave in the tables showed after injection, which is: passW0rD

Lesson 5:

1) First of all, try to register with the following username: Tom' AND '1'='1, and find that the user name is taken.
2) So we can use this method to check what tom's password is one at time by registering the following username: Tom' AND substring(password,1,1)='t
3) By checking all the remaining charactersm we found the password, thisisasecretfortomonly.

C. Injection Flaws: SQL Injection(mitigation)

Lesson 6:

Below is the code I used for this lesson:

```
try {
   Connection conn =
       DriverManager.getConnection(DBURL,
       DBUSER, DBPW);
   PreparedStatement stmt =
       conn.prepareStatement("SELECT * FROM
       users WHERE name = ?");
   stmt.setString(1, "Scott");
   stmt.executeUpdate();
} catch (Exception e) {
    System.out.println("Oops. Something went
        wrong!");
}
```

I believed there is no problem of this code but when I submit the code, it showed: ”error while writing TestClass: /TestClass.class”

D. Authentication Flaws: Password reset

Lesson 6:

I followed the link to change the request host from webwolf.ece.ubc.ca to webgoat.ece.ubc.ca and successfully catched the request from WebWolf. However, the value of path field in the request doesn’t contain the correct path for resetting the password. I suspect the server didn’t send the correct link to Tom for resetting password.

E. Cross-Site Scripting (XSS)

Cross Site Scripting, Cross Site Scripting (stored) and Cross Site Scripting (mitigation)

For the Cross-Site Scripting (XSS) module, every lesson within each sub-module had been solved and validated with the green icon. However, the overall sub-module did not reflect the green icon, and as such the report card also reflected that the sub-modules are uncompleted.

F. Access Control Flaws: Insecure Direct Object References

Lesson 3

1) Used the network tool in the development tools to capture the request after clicking ”View Profile”.
2) Found the following attributes in the response data section: color, name, role, size and userID.
3) The 2 hidden attributes are thus role and userId.

G. Access Control Flaws: Challenges: Admin password reset

This challenge has the same problem with the lesson 6 of password rest from authentication flaws section.

REFERENCES

[1] F. Stroud, “Dridex malware,” webopedia. [Online]. Available: https://www.webopedia.com/TERM/D/dridex-malware.html#. [Accessed: 05-Nov-2019].

[2] M. Sanghavi, “RIDEX and how to overcome it,” Symantec Official Blog, 30-May-2015. [Online]. Available: https://www.symantec.com/connect/blogs/dridex-and-how-overcome-it. [Accessed: 05-Nov-2019].