Digital Vengeance
Exploiting the Most Notorious C&C Toolkits

@professor__plum
I'M GONNA POP SOME SHELLS

GOT A FEW EXPLOITS IN MY POCKET
```bash
grep whoami /var/log/auth.log
plum
```
Disclaimer

- The views expressed herein do not necessarily state or reflect the views of my current or former employers.
- I am not responsible for any use or misuse of the information provided.
- Implementation of the information given is at your own risk.
The sophisticated attack

"... identified an extremely sophisticated cyber attack"
RSA

"Government and non-government entities are under constant attack by evolving and advanced persistent threats and criminal actors. These adversaries are sophisticated, well-funded, and focused."
Office of Personnel Management

"The threat is very persistent, adaptive and sophisticated – and it is here to stay,"
SWIFT

"The malware that was used would have slipped or probably got past 90% of internet defenses that are out there today in private industry"
Joseph Demarest, assistant director of the FBI’s cyber division

"hackers obtained data on tens of millions of current and former customers and employees in a sophisticated attack"
Anthem

“It is simply not possible to beat these hackers”
James A. Lewis Cybersecurity Expert at Center for Strategic and International Studies (CSIS)
Hacking back

- 36% of BH 2012 attendees surveyed said they engaged in some form of hacking back.
- Many feel justified in hacking back because their government isn’t doing enough to protect them.
- The ACDC would exempt victims from hacking laws when the aim is to identify the assailant, cut off attacks or discover stolen files.
Hacking back

- Most likely Illegal
- Little to no gain
- Much at risk
  - Liability
  - Reputation
  - Productivity
  - Escalation

GREETINGS PROFESSOR Falken
HELLO
A STRANGE GAME.
THE ONLY WINNING MOVE IS
NOT TO PLAY.
HOW ABOUT A NICE GAME OF CHESS?
“(ii) does not include conduct that—

“(I) destroys or renders inoperable information that does not belong to the victim that is stored on a computer of another;

“(II) causes physical or financial injury to another person;

“(III) creates a threat to the public health or safety; or

“(IV) exceeds the level of activity required to perform reconnaissance on an intermediary computer to allow for attribution of the origin of the persistent cyber intrusion;

“(C) the term ‘attacker’ means a person or an entity that is the source of the persistent unauthorized intrusion into the victim’s computer; and

“(D) the term ‘intermediary computer’ means a person or entity’s computer that is not under the ownership or control of the attacker but has been used to launch or obscure the origin of the persistent cyber-attack.”
“(i) means any measure—

“(I) undertaken by, or at the direction of, a victim; and

“(II) consisting of accessing without authorization the computer of the attacker to the victim’s own network to gather information in order to:

1) establish attribution of criminal activity to share with law enforcement and other United States Government agencies responsible for cybersecurity;

2) disrupt continued unauthorized activity against the victim’s own network; or

3) monitor the behavior of an attacker to assist in developing future intrusion prevention or cyber defense techniques, but;
>$ killall -s SIGKILL rants
RAT terminology

- Client
- Target
- Retaliator - one who returns assault in kind

- C2 Server
- Attacker
- Adversary

*icons credit Open Security Architecture
Sophisticated attack hit list

Top 10 malware counted by occurrence in #APT reports:
Poison Ivy
Gh0st RAT
PlugX
Xtreme RAT
Enfal
Derusbi
DarkComet
Shady RAT
NJRat
Wipbot
• Buffer overflow exploit by Andrzej Dereszowski
• Follow on work by Jos Wetzels
APT1 & Poison Ivy
Remote file download exploit by Shawn Denbow and Jesse Hertz

Follow on work by Jos Wetzels
```bash
$ chmod +r new_exploits
```
Xtreme RAT
Xtreme RAT Targets Israeli Government

Attackers targeting organizations across the globe are now opting to use a freely available remote access trojan called Xtreme RAT for their exploits.

On Monday, researchers at FireEye detailed in a blog post how the attack campaign, dubbed “Molerats,” has been ongoing since October 2011.

Molerats campaign turns to Xtreme RAT to target

Spyware malware found in Mexico's government

Researchers at cybersecurity firm Arbor Networks have located Xtreme RAT (Access Trojan) malware in the Mexican government's computer systems, a malicious activities found on its infrastructure.

Xtreme RAT cyberespionage targeted U.S., U.K.

Hackers dropping Zeus in favour of Xtreme RAT Trojan, reports FireEye

Now more powerful than banking Trojans, says FireEye
Xtreme Rat

- TCP connection starts with the string “myversion|3.x\r\n”
- C2 responds with “X\r\n”
- Alternatively Xtreme rat can use a fake HTTP request of the form GET /[0-9]{1,10}.functions
Remote file upload

Get ready to receive tool\bad.exe and save it to C:\temp\calc.exe

I’m ready to receive tool\bad.exe

Here is the [data]
Remote file download

- Win.ini (Sanity check)
- Event logs
- desktop.ini
- %SYSTEMROOT%\repair\SAM
- %SYSTEMROOT%\repair\system
- https://attackerkb.com/Windows/blind_files
PlugX / Korplug / Destory
The connection between the Plugx Chinese gang and the latest Internet Explorer ZeroDay

PlugX RAT Used to Gather Intel on Afghan, Russian Military: Report

PlugX – The Next Generation

I Know You Want Me - Unplugging PlugX

Takahiro Haruyama / Hiroshi Suzuki
Internet Initiative Japan Inc.
ret = DecodeMsgHeader(message, message);
if ( !ret )
{
    if ( msgHeader->size <= 0xF000u )
    {
        ...
    }
} else
{
    ShowMessage("PeDecodePacket");
    ret = 13;
}
return ret;
streamSize = TStreamGetSize();
if (streamSize < 16)
    return READ_MORE_DATA;

v6 = *global_struct;
result = DecodeMsgHeader(&msgHeader, v2->TStream->buffer);
if (!result)
{
    messageSize = msgHeader.size + 16;
    if (messageSize <= streamSize)
    {
        memcpy(Stackvar, msgHeader.size + 16, v2->TStream->buffer);
        v8 = v2->TStream;
        currentSize = TStreamGetSize();
        memcpy(v2->TStream->buffer, currentSize - messageSize, &v2->TStream->buffer[messageSize]);
        TStream = v2->TStream;
        newSize = TStreamGetSize();
        (*TStream->SetSize)(TStream->SetSize, newSize, newSize - messageSize);
        result = DecodePacket_(*global_struct, Stackvar);
    }
    else
    {
        result = READ_MORE_DATA;
    }
}
return result;
plum@Ballroom:~$ msfconsole
The PGconn, PGresult, and PGError constants are deprecated, and will be removed as of version 1.0.
You should use PG::Connection, PG::Result, and PG::Error instead, respectively.
Called from /opt/metasploit-framework/embedded/lib/ruby/gems/2.4.0/gems/activesupport-4.2.8/lib/active_support/dependencies.rb:274:in `block in require'

= metasploit v4.14.28-dev=
  +---[ 1663 exploits - 951 auxiliary - 293 post
  +---[ 486 payloads - 40 encoders - 9 nops
  +---[ Free Metasploit Pro trial: http://r-7.co/trymsp

msf >
Gh0st RAT

![Gh0st RAT Interface]

- **File Manager**
- **Screen Capture**
- **Keylogger**
- **Remote Shell**
- **System**
- **Webcam View**
- **Audio Capture**
- **Administrative Privileges**
- **Change Name**
- **Disconnect**
- **Select All**
- **Unselect**

**Connections**: 1

**IP**: 192.168.1.100

**Computer Name**: pluma-ad771c3ed7

**OS**: XP SP3 (Build 2600)

**CPU**: 3.092GHz

**Ping**: 10
Gh0st RAT

- Most notably identified by C2 traffic which start with the 5 byte marker “Gh0st” (or other 5 byte marker)

“The many faces of Gh0st Rat” — Snorre Fagerland
Remote file upload

Give me C:\Documents\user\file.doc so I can save it to targetX\file.doc

Here is the [data] so you can save it to targetX\file.doc
Remote file upload

Here is the [data]
so you can save it to C:\...\startup\backdoor.exe
DLL side load vulnerability

- Gh0st Server has a dependency on oledlg.dll
- Only imports one function
  - #8 OleUIBusyA(int)
- Return 1 and all is good
// 保存远程驱动器列表

memset(m_bRemoteDriveList, 0, sizeof(m_bRemoteDriveList));
memcpy(m_bRemoteDriveList, m_pContext->m_DeCompressionBuffer.GetBuffer(1), m_pContext->m_DeCompressionBuffer.GetBufferLen() - 1);
class CFileManagerDlg : public CDialog
{
  // Construction
  public:
  bool m_bIsStop;
  CString m_strReceiveLocalFile;
  CString m_strUploadRemoteFile;
  void ShowProgress();
  void SendStop();
  int m_nTransferMode;

  void ShowMessage(char *lpFmt, ...);
  CString m_Remote_Path;
  BYTE m_bRemoteDriveList[1024];
  CString GetParentDirectory(CString strPath);
  void OnReceiveComplete();

  CImageList* m_pImageList_Large;
  CImageList* m_pImageList_Small;

  int m_nNewItemBaseIndex;  // 新加的ICON

  ClientContext* m_pContext;
  CIOPServer* m_iocpServer;
  CString m_IPAddress;  //

Exploitation

- Control pointer to pointer
- Could use a information disclose vuln (if I had one)
- Thus, take the lazy man’s approach and heap spray
- DEP would break this but it also seems to break the EXE
Decode implant configs

- https://github.com/kevthehermit/RATDecoders
- Gh0st
- Xtreme Rat
- Poison Ivy
- DarkComet
- Many others
Malware Hunter
Finding the Command & Control Centers of Botnets across the Globe.

10+ RATs
3,000+ C2s identified
24/7 Coverage
Post exploitation

- Netstat
  - IP address of other victims
  - May show RDP connections in (or out)
- Walk FS looking for other hacking tools
- Install persistence
- Install keylogger
- Steal credentials
“He who is prudent and lies in wait for an enemy who is not, will be victorious.”

-- Sun Tzu, The Art of War
Thank you

@professor__plum