Digital Vengeance

Exploiting the Most Notorious C&C Toolkits

@professor___plum
<table>
<thead>
<tr>
<th>Login</th>
<th>Name</th>
<th>TTY</th>
<th>Idle</th>
<th>Login</th>
<th>Time</th>
<th>Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>plum</td>
<td>@Professor__Plum</td>
<td>pts/2</td>
<td>Sun</td>
<td>09:39</td>
<td>bc.symantec.com</td>
<td></td>
</tr>
<tr>
<td>plum</td>
<td>@Professor__Plum</td>
<td>pts/0</td>
<td>3yr</td>
<td>Tue</td>
<td>18:21</td>
<td>gin.bluecoat.com</td>
</tr>
<tr>
<td>plum</td>
<td>@Professor__Plum</td>
<td>pts/3</td>
<td>5yr</td>
<td>Fri</td>
<td>02:48</td>
<td>???.nsa.gov</td>
</tr>
</tbody>
</table>
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)
RAT terminology

- Client
- Victim
- Target

- C2 Server
- Attacker
- Victim
- Adversary

- Retaliator - one who returns assault in kind

*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
New work
Gh0st RAT

File Manager
Screen Capture
Keylogger
Remote Shell
System
Webcam View
Audio Capture
Administrate
miscellaneous
Change Name
Disconnect
Select All
Unselect

IP: 192.168.1.109
WAN: 192.168.1.109
OS: XP SP3 (Build 2600)
CPU: 3092MHz
Ping: 10
Webcam: --
Gh0st RAT

- Most notably identified by C2 traffic which start with the 5 byte marker “Gh0st” (or other 5 byte marker)
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_nNewIconBaseIndex; // 新加的ICON

   ClientContext* m_pContext;
   CIOCPServer* 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
PlugX / Korplug / Destory
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;
uint8_t v0 = *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);
        uint8_t v8 = v2->TStream;
        currentSize = TStreamGetSize();
        memcpy(v2->TStream->buffer, currentSize - messageSize, &v2->TStream->buffer[messageSize]);
        TStream = v2->TStream;
        newSizeSize = TStreamGetSize();
        (*TStream->SetSize)(TStream->SetSize, newSizeSize - messageSize);
        result = DecodePacket_(*global_struct, StackVar);
    } else
    {
        result = READ_MORE_DATA;
    }
}
return result;
plum@Ballroom:~$ msfconsole
The PGconn, PGrresult, 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 >
Xtreme RAT
Xtreme RAT Targets Israeli Government

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

Espionage malware used in attacks against Israel, as well as Syrian activists, in the last 18 months has been linked to a new attack against Israel’s Civil Administration, the governing body in the West Bank.

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.

Spyware malware found in Mexico’s government

Molerats campaign turns to Xtreme RAT to target orgs

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.

Espionage malware used in attacks against Israel, as well as Syrian activists, in the last 18 months has been linked to a new attack against Israel’s Civil Administration, the governing body in the West Bank.

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.

Spyware malware found in Mexico’s government

Molerats campaign turns to Xtreme RAT to target orgs

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.

Espionage malware used in attacks against Israel, as well as Syrian activists, in the last 18 months has been linked to a new attack against Israel’s Civil Administration, the governing body in the West Bank.

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.

Spyware malware found in Mexico’s government

Molerats campaign turns to Xtreme RAT to target orgs

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.

Espionage malware used in attacks against Israel, as well as Syrian activists, in the last 18 months has been linked to a new attack against Israel’s Civil Administration, the governing body in the West Bank.

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.

Spyware malware found in Mexico’s government

Molerats campaign turns to Xtreme RAT to target orgs

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.

Espionage malware used in attacks against Israel, as well as Syrian activists, in the last 18 months has been linked to a new attack against Israel’s Civil Administration, the governing body in the West Bank.

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.

Spyware malware found in Mexico’s government

Molerats campaign turns to Xtreme RAT to target orgs

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.

Espionage malware used in attacks against Israel, as well as Syrian activists, in the last 18 months has been linked to a new attack against Israel’s Civil Administration, the governing body in the West Bank.

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.

Spyware malware found in Mexico’s government

Molerats campaign turns to Xtreme RAT to target orgs

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.

Espionage malware used in attacks against Israel, as well as Syrian activists, in the last 18 months has been linked to a new attack against Israel’s Civil Administration, the governing body in the West Bank.

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.

Spyware malware found in Mexico’s government

Molerats campaign turns to Xtreme RAT to target orgs

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.

Espionage malware used in attacks against Israel, as well as Syrian activists, in the last 18 months has been linked to a new attack against Israel’s Civil Administration, the governing body in the West Bank.

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.

Spyware malware found in Mexico’s government

Molerats campaign turns to Xtreme RAT to target orgs

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.

Espionage malware used in attacks against Israel, as well as Syrian activists, in the last 18 months has been linked to a new attack against Israel’s Civil Administration, the governing body in the West Bank.

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.

Spyware malware found in Mexico’s government

Molerats campaign turns to Xtreme RAT to target orgs

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.

Espionage malware used in attacks against Israel, as well as Syrian activists, in the last 18 months has been linked to a new attack against Israel’s Civil Administration, the governing body in the West Bank.

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.

Spyware malware found in Mexico’s government

Molerats campaign turns to Xtreme RAT to target orgs

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.

Espionage malware used in attacks against Israel, as well as Syrian activists, in the last 18 months has been linked to a new attack against Israel’s Civil Administration, the governing body in the West Bank.

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.

Spyware malware found in Mexico’s government

Molerats campaign turns to Xtreme RAT to target orgs

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.

Espionage malware used in attacks against Israel, as well as Syrian activists, in the last 18 months has been linked to a new attack against Israel’s Civil Administration, the governing body in the West Bank.
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
Summary

- Remote file upload in Gh0St RAT C&C
  - Affected version 3.6
  - A carefully crafted packet could allow a remote attacker to upload remote files to the system. The attacker can also control the file name and location of where the remote file will be stored on the remote system, with which it may be possible to gain access to the system.
  - Authentication is not required to exploit the vulnerability

- Remote code execution in Gh0St RAT C&C
  - Affected version 3.6
  - A carefully crafted packet could allow a remote attacker to gain code execution thereby gaining access to the system.
  - Authentication is not required to exploit the vulnerability

- Remote code execution in PlugX
  - Affected versions 6.x - 7.x
  - A carefully crafted packet could allow a remote attacker to gain code execution thereby gaining access to the system
  - Authentication is not required to exploit the vulnerability

- Remote file download in XtremeRAT
  - Affected versions 3.6 - 3.7
  - A carefully crafted packet could allow a remote attacker to retrieve any file from the remote system
  - Authentication is not required to exploit the vulnerability
Thank you

@professor__plum