

Backdoor Use in Targeted Attacks

Dove Chiu, Shih-Hao Weng, and Joseph Chiu

Targeted Attack Defense Research Team



Contents

Introduction.....	1
Backdoor Techniques	2
Port Binding	2
Protection from Port Binding.....	4
Connect-Back Technique.....	4
Protection from the Connect-Back Technique	4
Connection Availability Abuse.....	4
Protection from Connection Availability Abuse	6
Legitimate Platform Abuse.....	7
Protection from Legitimate Platform Abuse	9
Common Service Protocol/File Header Abuse	9
Protection from Common Service Protocol/File Header Abuse	10
Protocol/Port Listening	10
Protection from Protocol/Port Listening	13
Custom DNS Lookup Use	13
Protection from Custom DNS Lookup Use	14

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Port Reuse..... 14

 Protection from Port Reuse 15

Conclusion..... 15

References 16



Introduction

Backdoors—applications that open computers to remote access—play a crucial role in targeted attacks.¹ Often initially used in the second (point of entry) or third (command-and-control [C&C]) stage of the targeted attack process, backdoors enable threat actors to gain command and control of their target network.²

Backdoors allow attackers to establish a connection with their target network while evading detection. In fact, research reveals that many of the backdoors used in targeted attacks have been especially designed with the ability to bypass any kind of intrusion detection system (IDS).³

There are various techniques backdoors use to enable attackers to gain command and control of their target network. Understanding them can help IT administrators more effectively detect their presence and protect the networks they manage from targeted attacks.

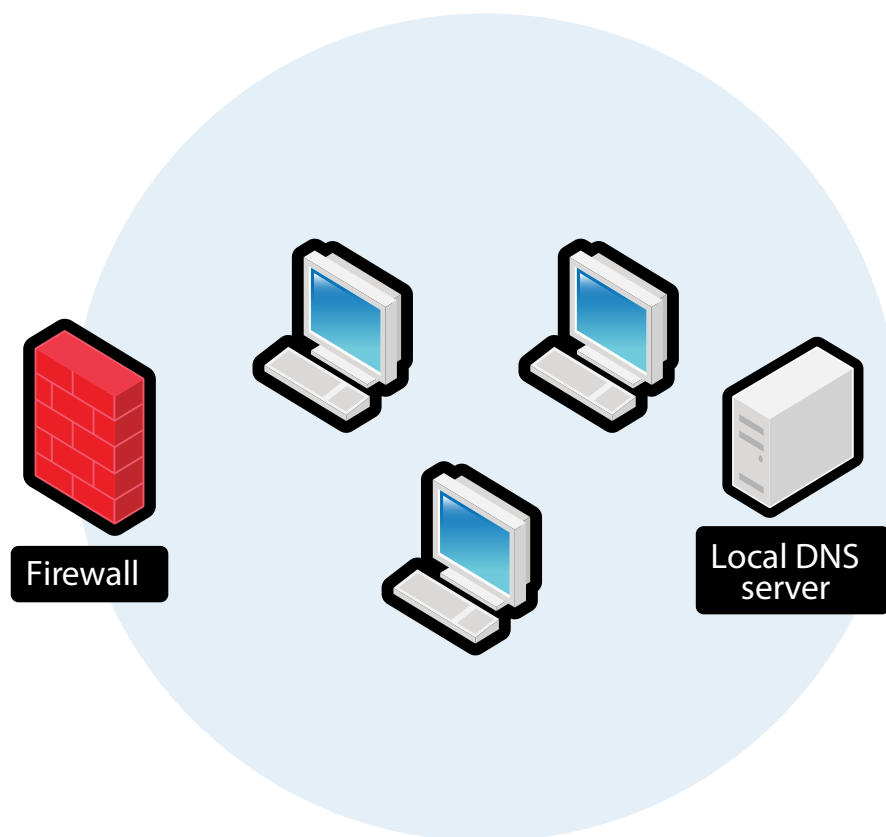


Figure 1: Typical corporate network setup

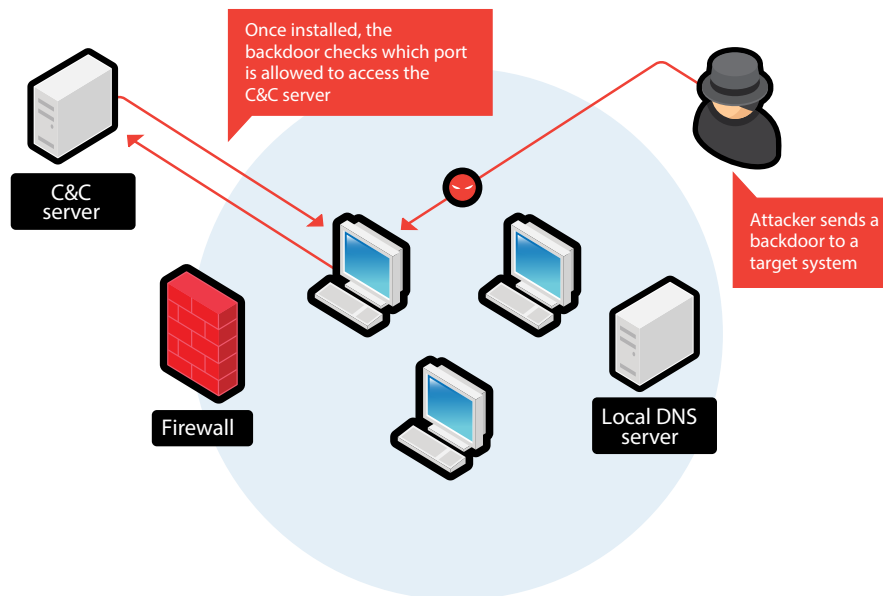


Figure 2: Typical targeted attack on a corporate network

Backdoor Techniques

Port Binding

Port binding—configuring information to determine where and how messages are sent or received—was commonly seen before firewalls became part of most corporate networks.⁴ Back then, most servers had public IP addresses, making them vulnerable to attacks.

This technique could allow attackers to configure a backdoor to directly communicate or “bind” with a specific server port, allowing them to more easily take control of the affected server. Once a connection is established, the backdoor can spawn a simple shell to execute commands.

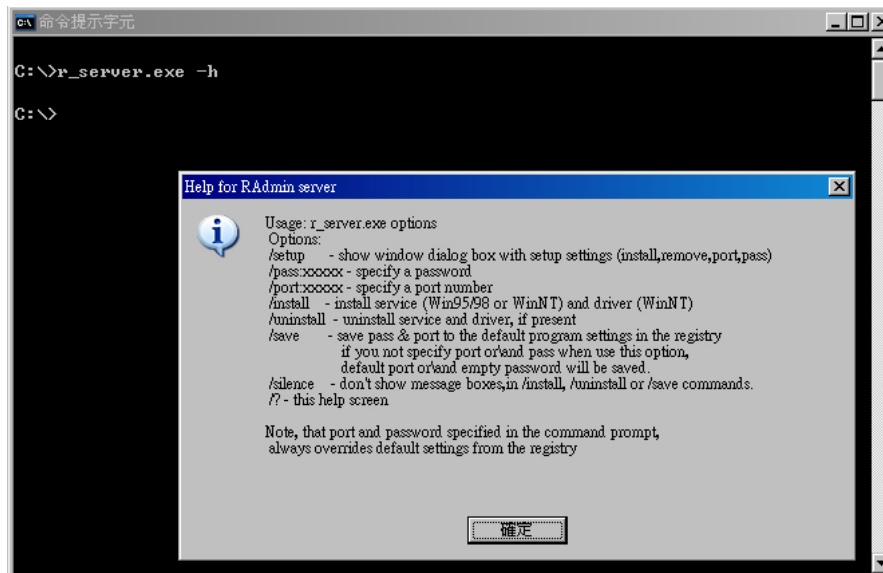


Figure 3: Modified Radmin® Server software that shows a command prompt instead of the usual graphical user interface (GUI)

A popular application that uses port binding is Radmin Server.⁵ Although originally designed as a piece of remote access software for technical support purposes, attackers have modified Radmin Server components to infiltrate target networks.⁶ They typically modify the software so it would not display a GUI.

Although firewalls are now basic components of corporate networks, those that do not employ them remain vulnerable to port binding abuse.

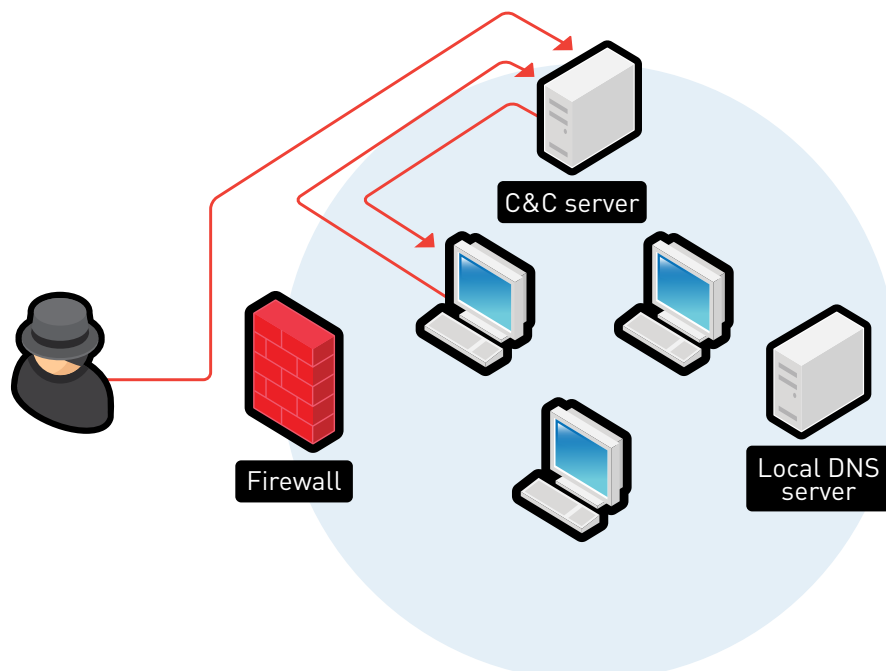


Figure 4: How port binding works

Protection from Port Binding

IT administrators can prevent attacks via port binding by putting up a firewall that can block incoming connections from a backdoor.

Connect-Back Technique

A common means by which attackers bypass firewalls is via the so-called “connect-back” technique.⁷ Attackers use backdoors to connect victims’ systems to their C&C server and vice versa via ports that are not blocked by corporate firewalls. This allows them to remain undetected in target networks.

In order to bypass corporate firewalls, attackers must deliver a backdoor to their target network so they can connect systems to their C&C server and vice versa. This requires bypassing other protection means such as anti-malware solutions. Attackers often use emails to deliver backdoors to targets.⁸ It is also common for attackers to compromise and use servers with public IP addresses as C&C servers to better hide their tracks.

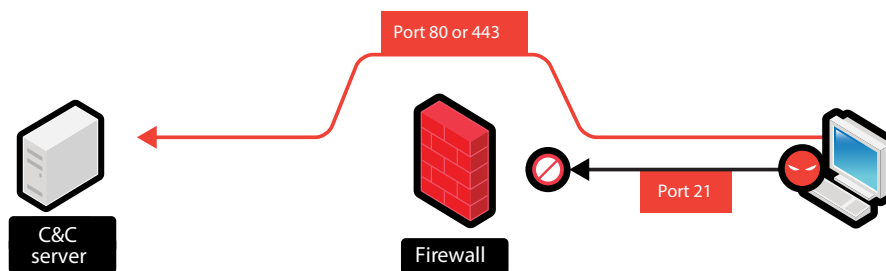


Figure 5: How the connect-back technique works

Protection from the Connect-Back Technique

Firewall and IDS usage on both the network and endpoint fronts can help IT administrators protect their organizations from attacks using the connect-back technique. Continuous monitoring for suspicious connections to external IP addresses for blocking purposes and conducting investigations, if necessary, also help.

Email scanning and/or filtering solutions to block emails with malicious attachments or that contain malicious URLs also help. Examples of these solutions include Trend Micro™ InterScan™ Messaging Security, Trend Micro Deep Discovery, and Trend Micro ScanMail™ Suite for Microsoft® Exchange™.^{9, 10, 11}

Connection Availability Abuse

Attackers typically use several malware to infiltrate and maintain persistence in as well as to obtain confidential information out of target networks. An example of this is an attack in which the malware used to infiltrate a network differed from the malware that remained in the network to steal information.¹²

The initial malware—the “first-line backdoor”—primarily acts as a downloader of another malware—the “second-line backdoor”—that steals information. In such an attack, the first-line backdoor ensures that the second-line backdoor is installed in target systems while evading detection. In most cases, attackers use different C&C servers for their first- and second-line backdoors so that these would remain independent of each other.

```

Private Function getIP()
    Dim strIPAddr
    If Request.ServerVariables("HTTP_X_FORWARDED_FOR") = "" OR InStr(Request.ServerVariables("REMOTE_ADDR")) = 0 Then
        strIPAddr = Request.ServerVariables("REMOTE_ADDR")
    Else
        strIPAddr = Mid(Request.ServerVariables("HTTP_X_FORWARDED_FOR"), InStr(Request.ServerVariables("HTTP_X_FORWARDED_FOR"), ",") + 1, Len(Request.ServerVariables("HTTP_X_FORWARDED_FOR")))
    End If
    strIPAddr = Trim(Mid(strIPAddr, 1, 30))
    If strIPAddr = "" Then strIPAddr = Request.ServerVariables("REMOTE_ADDR")
    getIP = strIPAddr
End Function

Set fso = Server.CreateObject("Scripting.FileSystemObject")
ByteCount = Request.TotalBytes
BinRead = Request.BinaryRead(ByteCount)
fso.open getIP() & "32-blank.exe", 8192, True, 4
fso.write BinRead
fso.close
response.BinaryWrite fso.ReadAll

```

Figure 6: Sample server script used as a second-line backdoor in a targeted attack

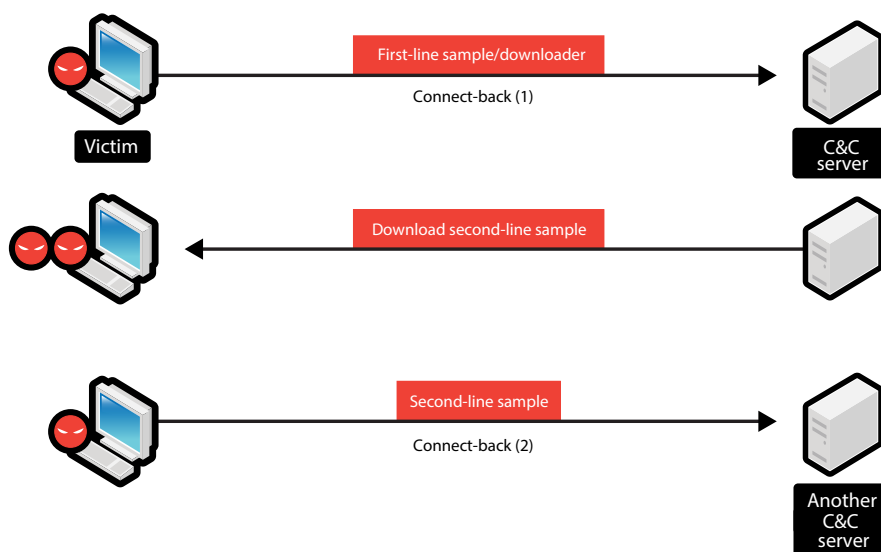


Figure 7: How first- and second-line backdoors work with each other in a targeted attack

To ensure that the final payload is executed on the target system, attackers constantly check for connection to their C&C servers through a ping or Netcat—a network utility that reads and writes data across network connections.¹³

In some instances, however, establishing a connection with C&C servers does not mean the attackers can also successfully bypass installed IDSs on networks, if any. Backdoors built with features similar to Netcat such as TSPY_DESLOC.AA have been used in attempts to establish C&C server connections while bypassing IDS detection.¹⁴

No.	Time	Source	SrcPort	Destination	DestPort	Protocol	Length	Info
2	2014-05-29 12:00:21.785754000	192.168.0.123	1196	1196.1.3.7	80	TCP	62	netmagic > http [SYN] Seq=361701934
7	2014-05-29 12:00:22.785632000	1.3.3.7	80	192.168.0.123	1196	TCP	62	http > netmagic [SYN, ACK] Seq=1 Ack=
8	2014-05-29 12:00:22.786597000	192.168.0.123	1196	1.3.3.7	80	TCP	54	netmagic > http [ACK] Seq=361701935
9	2014-05-29 12:00:22.793223000	192.168.0.123	1196	1.3.3.7	80	TCP	70	[TCP segment of a reassembled PDU]

Figure 8: The backdoor accesses C&C servers while attempting to evade IDS detection via the additional parameter inserted to its code (screenshot was taken while running the backdoor in a simulated network environment)

In attacks that use this technique, the attackers can conveniently switch C&C servers to check the following on the target network:

- Is the C&C server's IP address or domain name blacklisted?
- Is the target port protected by a firewall?
- Is the C&C server's network signature blocked?

Successfully circumventing the above-mentioned protections allows the attackers to establish a temporary connection to the target system to execute routines such as transferring files.

Attackers also use single-thread backdoors to infiltrate networks though this technique has limitations. While transferring files, such backdoors cannot do anything else such as evading detection. So the bigger the size of the file being transferred, the longer it takes for the transfer and the greater the chances of detection.

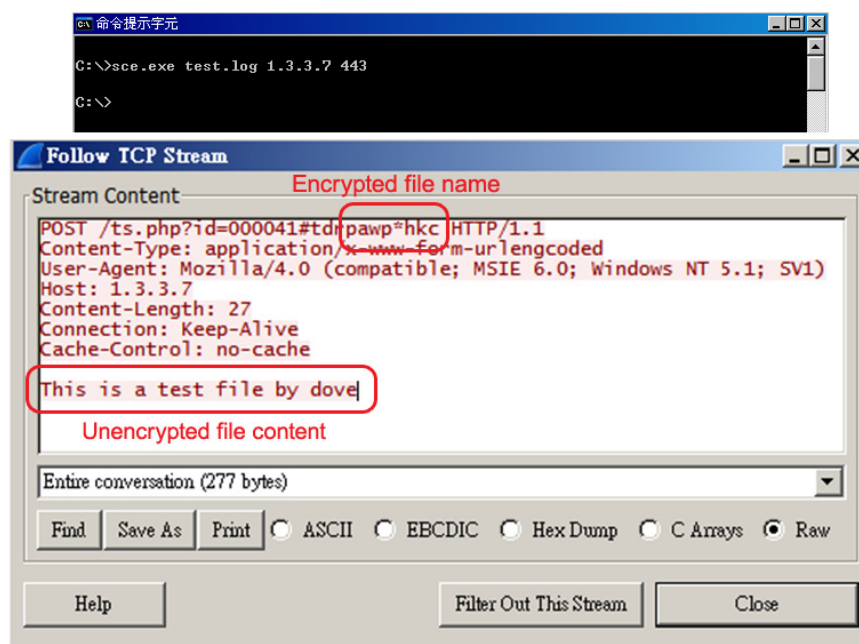


Figure 9: The backdoor process attempting to transfer a file to a C&C server through port 443 (screenshot was taken while running the backdoor in a simulated network environment)

Protection from Connection Availability Abuse

Using a security solution that monitors network patterns such as Trend Micro Deep Discovery is an effective form of protection from attacks that use this technique. Note, however, that some backdoor patterns are harder to detect than others. Some backdoors do not exhibit network patterns and look like normal HTTP protocol, which could lead to false alarms.

Legitimate Platform Abuse

Since bypassing security solutions is a primary goal of the backdoors used in targeted attacks, abusing legitimate platforms for malicious activities is not uncommon. A good example of this technique is an incident where blogs are abused to store C&C server information.¹⁵

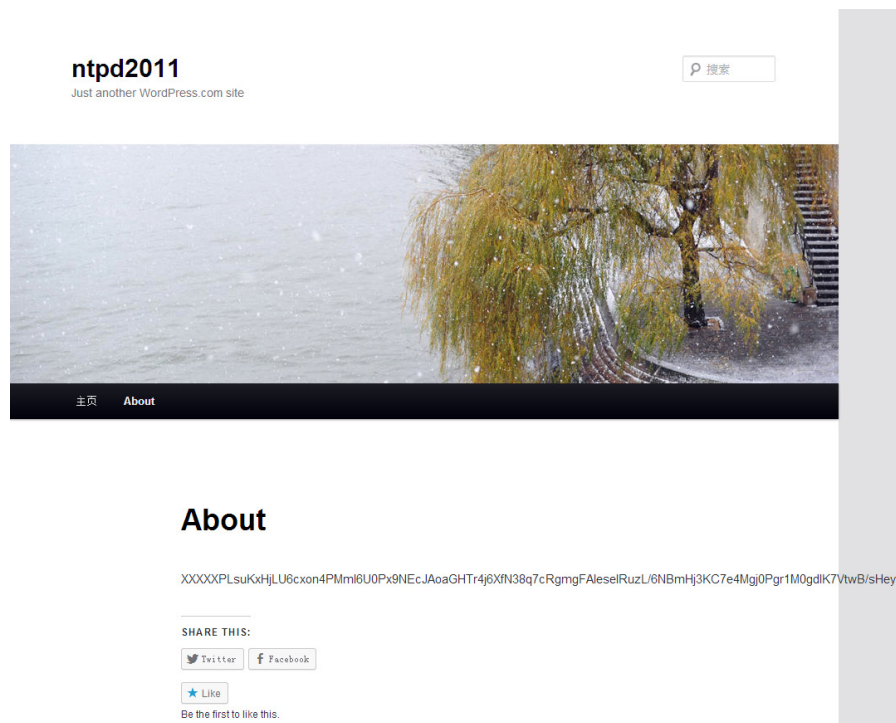


Figure 10: Blog page that contains cipher text that, when decrypted, shows the C&C server IP address to access and the port to use

```

C:\>CnCDDecoder.exe "ef5pK02+cAGDgt6vfZLMjDtqtP0nH/0oaGHTTr4j6xFN38q7cRgm62R1xIaoFUaYS149zJd0YBun0Fw0nsRnEY4M1bjwIvsnXDunCrWjXJAYLMMWE10o+JtImjqNZbmu42bdjmj1TRqvIQebl7FKQo2Eq6bMNRfIEzZUyLBwFMbgSfrnuvAikoZgJofyRK/7JzAq3J7lotXu2AGG+tnAM.le+n6xM6IABwtvdCzdFgayLyFSa1JLYCYz0dhnm0aa6Uho+50bCGBz0hscURc.j0wX/"
65 61 2E 74 6F 79 74 68 69 65 a.toythie
76 65 73 2E 63 6F 6D 00 00 00 00 00 00 00 00 00 ves.com
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
BB 01 00 00 50 00 00 00 00 00 00 00 00 77 77 77 2E P www.
52 2E 71 68 69 67 68 2E 63 6F .qhigh.co
6D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 m
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
50 00 00 00 00 00 00 00 77 77 77 2E P www.
64 64 6E 73 2E 75 73 00 00 00 00 00 00 00 00 ddns.us
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 69 6D 61 70 73 65 72 76 65 72 2E 6D P
61 69 6C 2E 2E 74 77 00 00 00 00 00 00 00 00 imapserver.m
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ail. .tw
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 BB 01 00 00 50 00 00 00 00 00 00 00 P
2E 77 65 62 6D 61 69 6C 2E .webmail.
67 67 65 73 2E 74 77 00 00 00 00 00 00 00 00 gies.tw
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
BB 01 00 00 50 00 00 00 00 00 00 00 00 10 0E 00 00 P
C:\>

```

Figure 11: List of C&C server IP addresses when the cipher text is decrypted

In this attack type, the backdoor first accesses the blog URL to obtain the cipher text. It then decrypts the text and accesses any of the decrypted IP addresses in the C&C server list. The attackers can easily change the IP addresses in the list by modifying the cipher text in the blog, allowing them to hide their tracks.

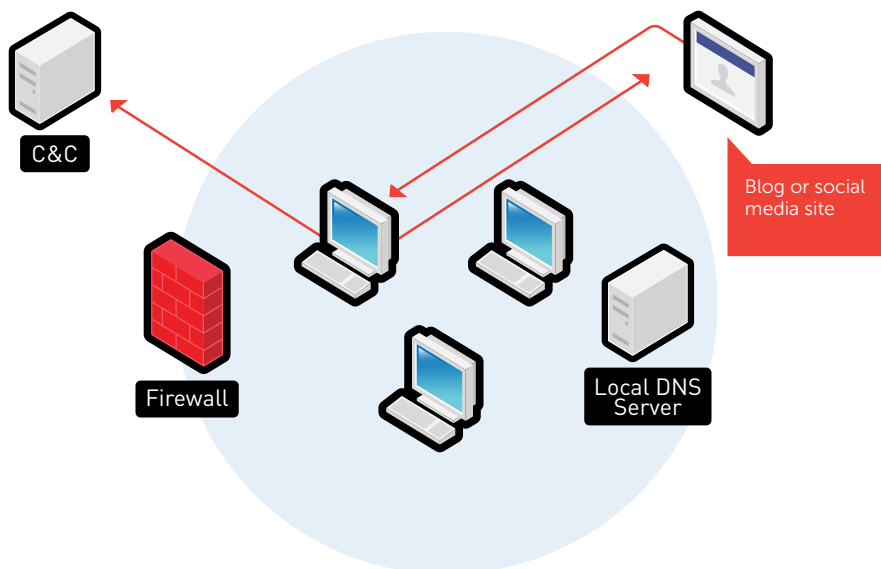


Figure 12: How legitimate platform abuse works

Protection from Legitimate Platform Abuse

Blocking traffic to and from legitimate platforms such as blogs is tricky because doing so can result in false alarms. To prevent such an attack, it is necessary to decrypt the cipher text in order to obtain and block the domains it points to. Detection at the network level could also be accomplished by using network signatures although this could also result in false alarms.

Common Service Protocol/File Header Abuse

Attackers also abuse legitimate protocols such as those of instant messengers (IMs) and free email services to hide their tracks. We have, in fact, seen the protocols of IMs such as Windows® Live Messenger and Ajax IM as well as of email services such as Gmail™ abused by backdoors like BKDR_DESCLOC.A in targeted attacks.

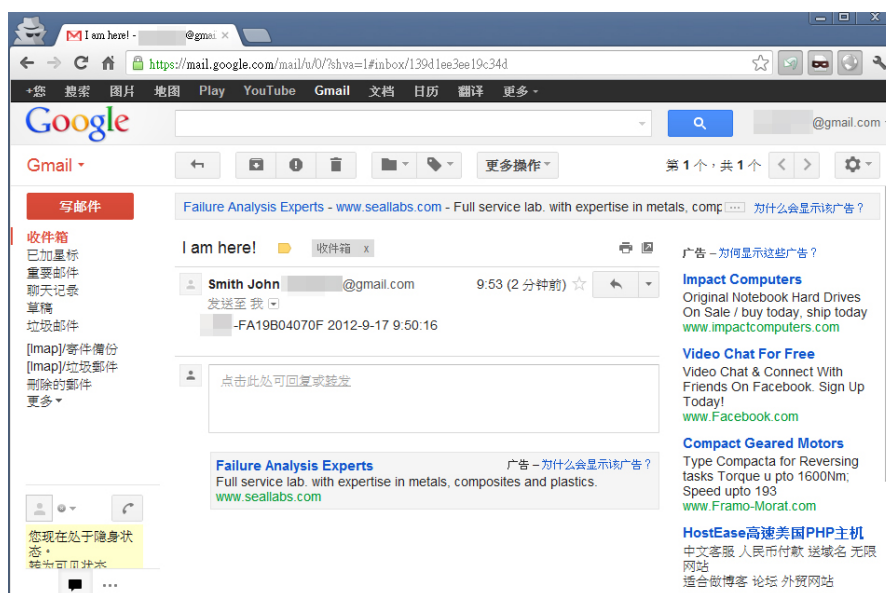


Figure 13: Report the backdoor sends to the attackers via Gmail

An example of this is Terminator, a backdoor detected as FAKEM, which attempts to emulate the first 32 bytes of common legitimate protocol/file headers to evade detection, albeit unsuccessfully.¹⁶

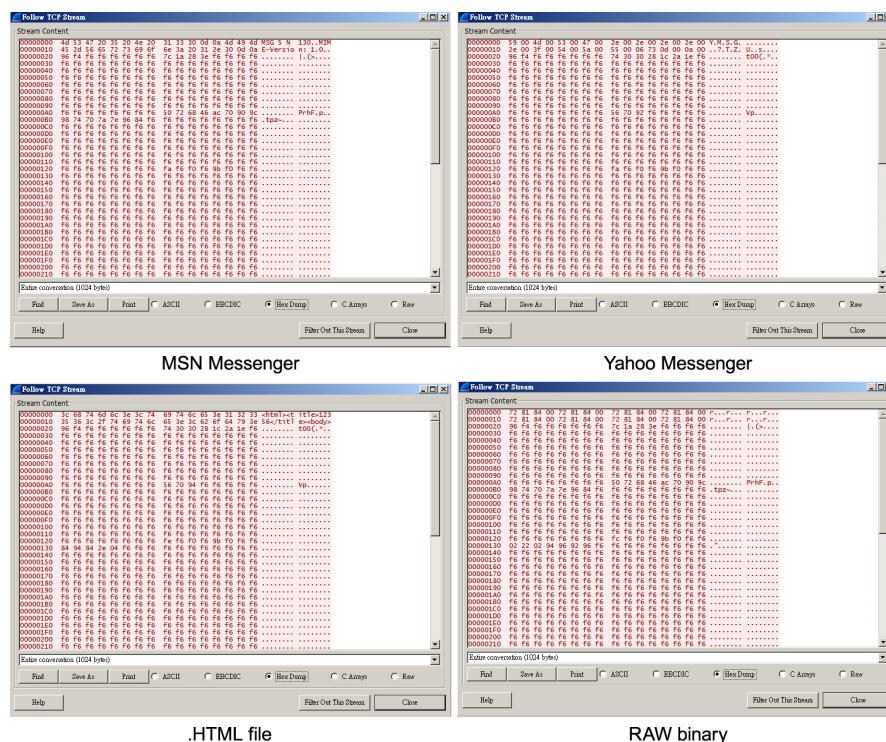


Figure 14: Four kinds of header that Terminator emulates for C&C communication purposes

Backdoors in attacks that use this technique are very difficult to detect if they emulate the entire header of a protocol/file. This would require a fully knowledgeable attacker. Such backdoors could also easily become unstable since the slightest error in the header could render them unusable.

Protection from Common Service Protocol/File Header Abuse

Because this could allow attackers to emulate legitimate network traffic, attacks that use this technique are impossible to detect at the network level. The only way to detect backdoors with this capability is through the use of an effective anti-malware solution such as Trend Micro OfficeScan.

Protocol/Port Listening

Apart from changing C&C server URLs, ports, IP addresses, and domain names, attackers also modify the protocols they use for communication to evade detection. A PlugX variant, for instance, uses User Datagram Protocol (UDP) instead of the usual Transmission Control Protocol (TCP) to access its C&C server.¹⁷ This backdoor had a simplified TCP header at the beginning of data transmission to prevent loss, however, since UDP does not have three-way handshake and congestion control capabilities. Handshaking allows the backdoor to verify the connection between two systems.¹⁸

51	2013-01-10 14:45:59.499128	192.168.0.101	1036 1.3.3.7	4002 UDP	66 Source port: nsstp Destination port: p
52	2013-01-10 14:45:59.499192	192.168.0.101	1036 1.3.3.7	4002 UDP	66 Source port: nsstp Destination port: p
53	2013-01-10 14:45:59.499238	192.168.0.101	1036 1.3.3.7	4002 UDP	66 Source port: nsstp Destination port: p
54	2013-01-10 14:45:59.518791	192.168.0.101	1036 1.3.3.7	4002 UDP	66 Source port: nsstp Destination port: p
55	2013-01-10 14:45:59.518880	192.168.0.101	1036 1.3.3.7	4002 UDP	66 Source port: nsstp Destination port: p
56	2013-01-10 14:45:59.518951	192.168.0.101	1036 1.3.3.7	4002 UDP	66 Source port: nsstp Destination port: p
57	2013-01-10 14:46:01.077453	192.168.0.101	1036 1.3.3.7	4002 UDP	66 Source port: nsstp Destination port: p
58	2013-01-10 14:46:01.077538	192.168.0.101	1036 1.3.3.7	4002 UDP	66 Source port: nsstp Destination port: p
59	2013-01-10 14:46:01.077584	192.168.0.101	1036 1.3.3.7	4002 UDP	66 Source port: nsstp Destination port: p
60	2013-01-10 14:46:02.642884	192.168.0.101	1036 1.3.3.7	4002 UDP	66 Source port: nsstp Destination port: p
61	2013-01-10 14:46:02.642946	192.168.0.101	1036 1.3.3.7	4002 UDP	66 Source port: nsstp Destination port: p
62	2013-01-10 14:46:02.642996	192.168.0.101	1036 1.3.3.7	4002 UDP	66 Source port: nsstp Destination port: p
71	2013-01-10 14:46:04.219557	192.168.0.101	1036 1.3.3.7	4002 UDP	66 Source port: nsstp Destination port: p
72	2013-01-10 14:46:04.219615	192.168.0.101	1036 1.3.3.7	4002 UDP	66 Source port: nsstp Destination port: p
73	2013-01-10 14:46:04.219662	192.168.0.101	1036 1.3.3.7	4002 UDP	66 Source port: nsstp Destination port: p
77	2013-01-10 14:46:05.781198	192.168.0.101	1036 1.3.3.7	4002 UDP	66 Source port: nsstp Destination port: p
78	2013-01-10 14:46:05.781267	192.168.0.101	1036 1.3.3.7	4002 UDP	66 Source port: nsstp Destination port: p

Frame 57: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)		0000 00 10 20 30 40 50 60 29 7e 19 96 08 00 45 00 .. ODP...)....E.
Ethernet II, Src: Vmware_7e:19:96 (00:0c:29:7e:19:96), Dst: Handfield_30:40:50 (00:0c:29:7e:19:96)		0010 00 34 00 46 00 00 80 11 75 5c c0 a8 00 65 01 03 ..4.F.... u....e.
Internet Protocol Version 4, Src: 192.168.0.101 (192.168.0.101), Dst: 1.3.3.7 (1.3.3.7)		0020 03 07 04 0c 0f a2 00 20 c1 28 30 00 02 00 00 00 00000000
User Datagram Protocol, Src Port: nsstp (1036), Dst Port: pxc-srvr-ft (4002)		0030 0f a2 01 03 03 07 00 04 00 00 00 00 00 00 00 00 00000000
Data (24 bytes)		0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00000000

Figure 15: PlugX uses UDP to access its C&C server

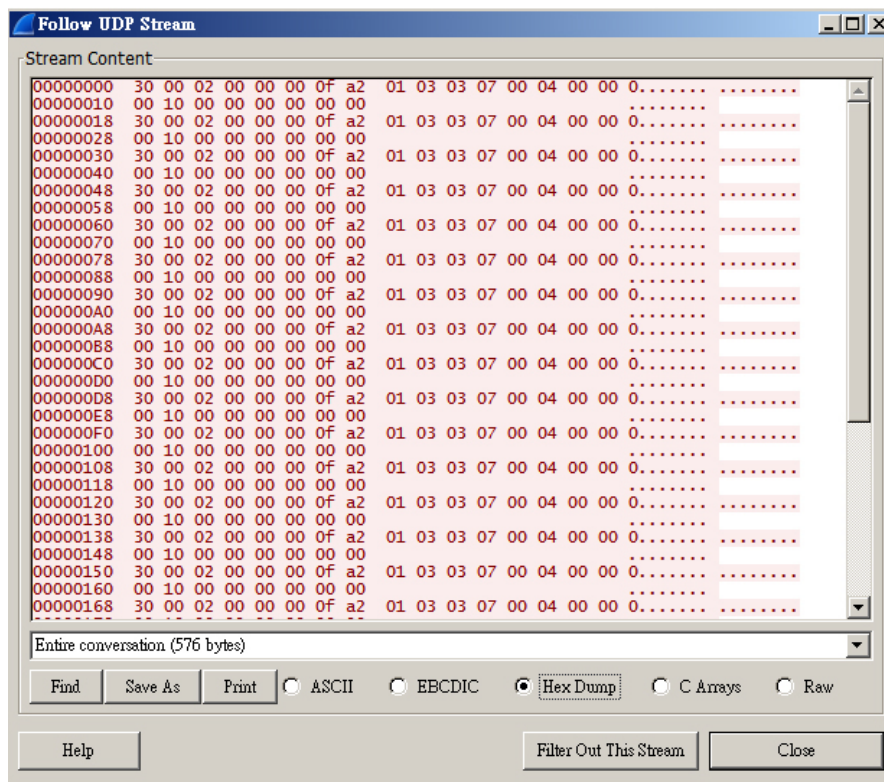


Figure 16: PlugX implements part of its TCP header in UDP

Samples found do not only use UDP to access the C&C server but also use Internet Control Message Protocol (ICMP). This particular option has been built into the PlugX controller, which allows attackers to specify which C&C server to access and which protocol to use among TCP, HTTP, UDP, and ICMP.

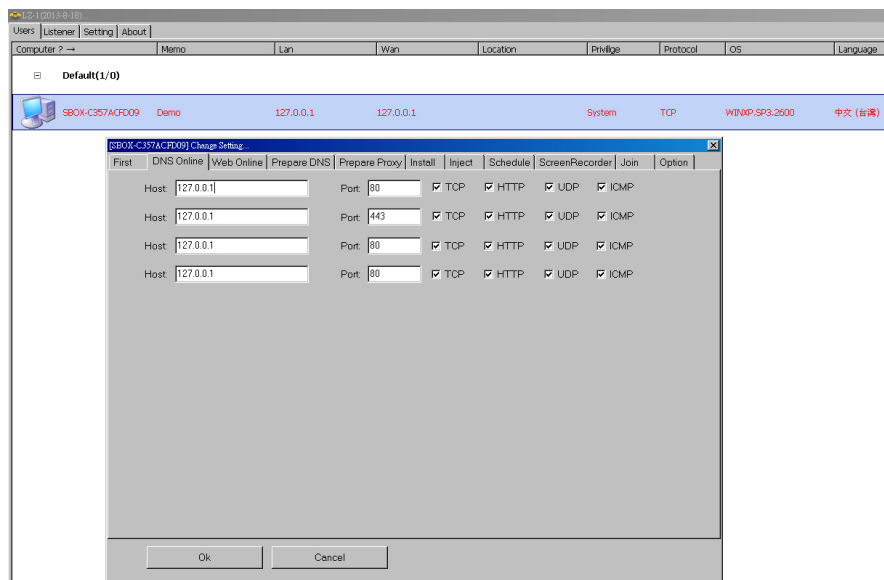


Figure 17: PlugX backdoor's connect-back settings

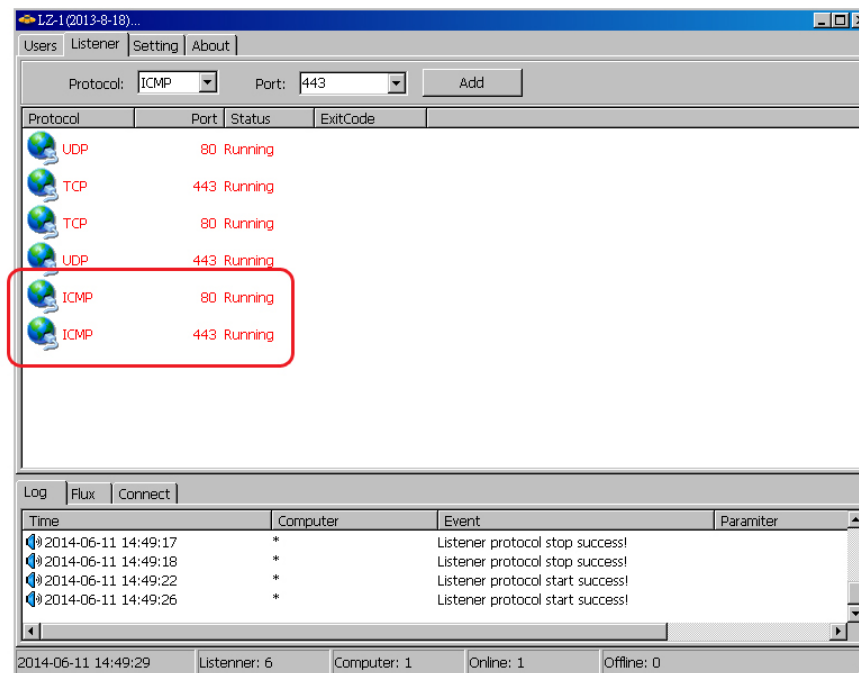


Figure 18: PlugX's controller can listen to several ports and for protocols at the same time so it can better choose which protocol and port to use for C&C communication

Protection from Protocol/Port Listening

Blocking backdoors that can use various protocols and ports to communicate with their C&C servers require certain firewall settings to ensure that only the necessary ports are open to certain protocols. IT administrators could, for instance, block all ICMP traffic from coming into or going out of their networks. Even though this is a secure setup, it may also cause significant inconvenience to users. However, since Domain Name System (DNS) lookups use UDP port 53, it is often left open as backup when the local DNS server goes offline.

Custom DNS Lookup Use

Blacklist implementation in a network environment allows firewalls to block access to C&C server IP addresses. Access to C&C server domain names, however, cannot be blocked by firewalls since these do not block traffic until after a DNS lookup is triggered. Blocking queries to the DNS server is thus done instead.

To bypass security measures, attackers trigger a custom DNS lookup query to Web services to divert traffic going to the real C&C server IP address.

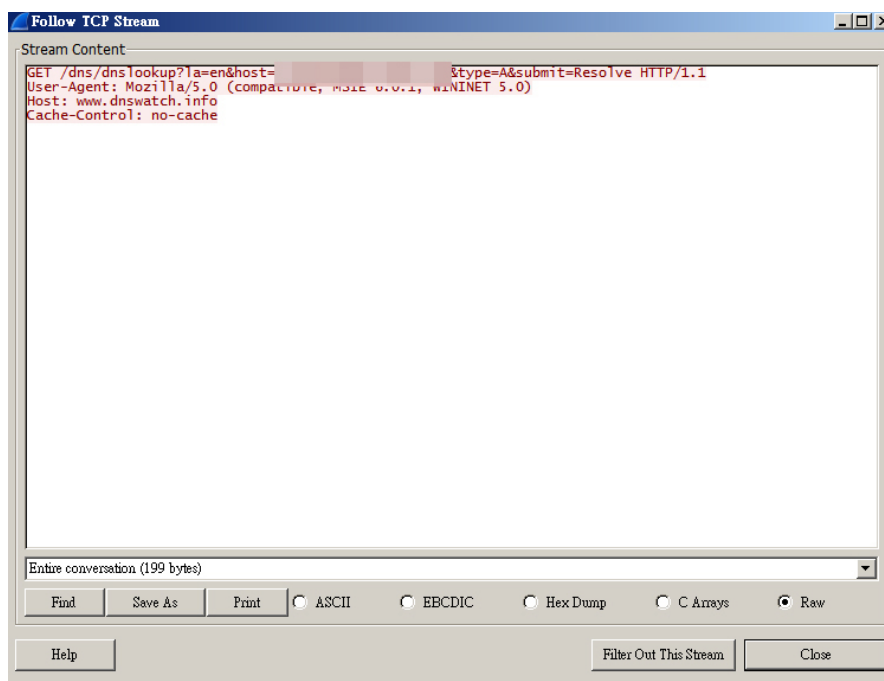


Figure 19: Custom DNS lookup query the backdoor sends to a Web service

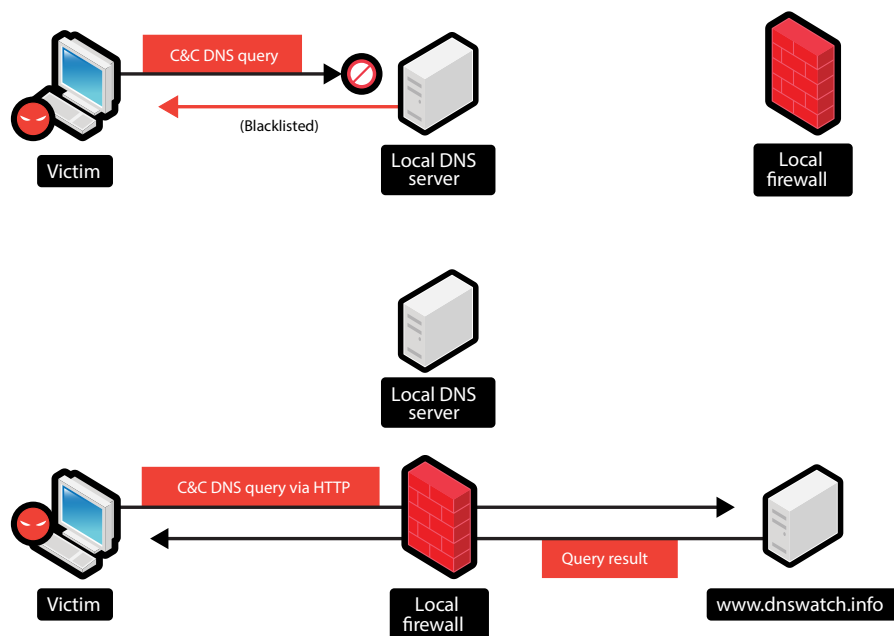


Figure 20: How normal (top) and custom (bottom) DNS lookup queries work

Even though this technique appears simple, it can allow attackers access to C&C servers even if their domain names are already being blocked by the target's local DNS server. They can also choose when to open the servers to connections by modifying their DNS records to only access the IP addresses, 0.0.0.0 and 127.0.0.1, when these are not in use to evade detection.

Protection from Custom DNS Lookup Use

Since custom DNS servers are not malicious in nature, it is not possible to block access to them when backdoors attempt to access customized server domain names instead of C&C server IP addresses. IT administrators have to determine the IP addresses the customized domain names point to and block access to them instead via firewalls and IDSs.

Port Reuse

Port reuse requires the use of a kernel mode, also known as “Ring0,” driver to execute routines.¹⁹ Backdoors with this capability use the Network Driver Interface Specification (NDIS) or Windows Filtering Platform (WFP) to listen to already-open ports on a target system. Attackers who use such backdoors can reuse any open port without causing running services to change.

Address	Ordinal	Name	Library
000000...		FwpsInjectNetworkSendAsync0	fwpkclnt
000000...		FwpsInjectionHandleCreate0	fwpkclnt
000000...		FwpsInjectionHandleDestroy0	fwpkclnt
000000...		FwpsQueryPacketInjectionState0	fwpkclnt
000000...		FwpsInjectNetworkReceiveAsync0	fwpkclnt

Figure 21: Ring0 backdoor import functions related to packet injection²⁰

Using a kernel mode driver in 32- and 64-bit Windows systems allows such backdoors to filter signatures, execute commands, and reply with results. Attackers, however, need to steal signed certificates for their backdoors on Windows 7 so these would run on 64-bit systems.

Backdoors with port reuse capability specifically in Ring3 can also be implemented in user mode. If raw sockets to filter backdoor connections are used in user mode, a process could trigger detection. Attacks where the backdoor is registered as a Service Provider Interface (SPI) process leave evidence in the system registry and could be detected.

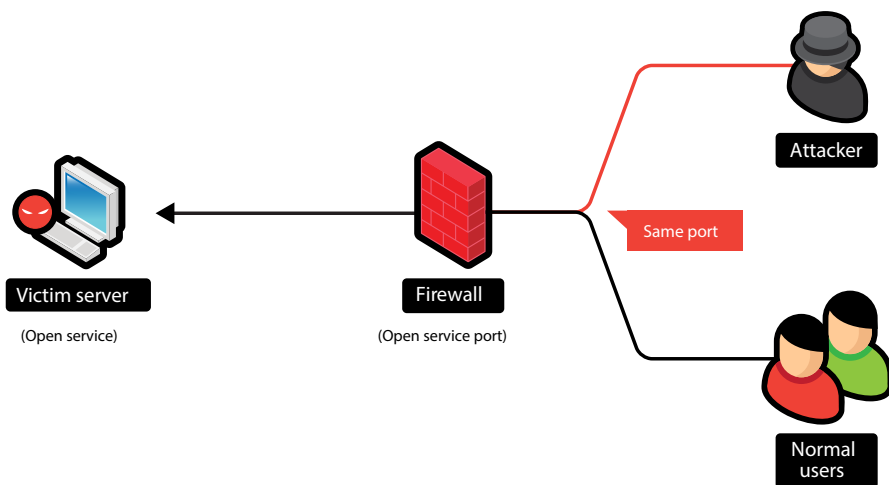


Figure 22: How port reuse works

Protection from Port Reuse

Backdoors that have port reuse capability are difficult to detect. Endpoint security solutions such as anti-malware or file/process-monitoring products (e.g., Trend Micro™ Titanium™ Security and OfficeScan™) can be helpful as well as network IDSs and intrusion prevention systems (IPSs).

Conclusion

Attackers are constantly improving their tactics. As such, apart from protecting systems and networks against targeted attacks, organizations must also make sure that their IT administrators/teams stay aware and updated on security.

The methods of protection described in this paper are not fool-proof but they can effectively reduce infiltration risks. Unfortunately, IT administrators are at a disadvantage compared to attackers. IT administrators need to know every possible means by which their networks can be breached and must then find a way to protect it. Attackers, on the other hand, only need to find a single weakness to exploit in a target network to succeed. The weakest point—the human factor—makes awareness a critical component of securing networks.

In sum, IT administrators must not only have sufficient know-how and expertise on securing their organizations' networks but must also be equipped with the right solutions and tools that can timely and effectively detect potentially malicious activities in their networks.

References

- [1] Trend Micro Incorporated. (2014). *Threat Encyclopedia*. “Backdoor.” Last accessed July 10, 2014, <http://about-threats.trendmicro.com/us/definition/backdoor>.
- [2] Trend Micro Incorporated. (2012). *Threat Encyclopedia*. “Detecting the Enemy Inside the Network: How Tough Is It to Deal with APTs?” Last accessed July 10, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_apr-primr.pdf.
- [3] Wikimedia Foundation Inc. (July 2, 2014). *Wikipedia*. “Intrusion Detection System.” Last accessed July 10, 2014, http://en.wikipedia.org/wiki/Intrusion_detection_system.
- [4] Microsoft. (2014). *Microsoft Developer Network*. “Port Bindings.” Last accessed July 10, 2014, <http://msdn.microsoft.com/en-us/library/aa578247.aspx>.
- [5] Famatech. (2014). *Radmin*. “Radmin 3 Remote Control Software—Radmin Server.” Last accessed July 10, 2014, <http://www.radmin.com/radmin/rserver.php>.
- [6] Trend Micro Incorporated. (2014). *Threat Encyclopedia*. “HKTL_RADMIN.” Last accessed July 10, 2014, http://about-threats.trendmicro.com/us/malware/HKTL_RADMIN.
- [7] Wikimedia Foundation Inc. (June 6, 2014). *Wikipedia*. “Shellcode.” Last accessed July 10, 2014, <http://en.wikipedia.org/wiki/Shellcode>.
- [8] Trend Micro Incorporated. (2012). *Threat Encyclopedia*. “Targeted Attack Entry Points: Are Your Business Communications Secure?” Last accessed July 10, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/business/tlp_targeted_attack_entry_points.pdf.
- [9] Trend Micro Incorporated. (2014). *Trend Micro InterScan Messaging Security*. Last accessed July 10, 2014, <http://www.trendmicro.com/us/enterprise/network-security/interscan-message-security/>.
- [10] Trend Micro Incorporated. (2014). *Trend Micro Deep Discovery Advanced Network Security*. Last accessed July 10, 2014, <http://www.trendmicro.com/us/enterprise/security-risk-management/deep-discovery/>.
- [11] Trend Micro Incorporated. (2014). *Trend Micro ScanMail Suite for Microsoft Exchange*. Last accessed July 10, 2014, <http://www.trendmicro.com/us/enterprise/network-web-messaging-security/scanmail-microsoft-exchange/>.
- [12] Trend Micro Incorporated. (May 12, 2014). *TrendLabs Security Intelligence Blog*. “Targeted Attack Against Taiwanese Agencies Used Recent Microsoft Word Zero-Day.” Last accessed July 10, 2014, <http://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attack-against-taiwanese-agencies-used-recent-microsoft-word-zero-day/>.
- [13] Giovanni Giacobi. (November 1, 2006). *The GNU Netcat Project*. “What Is Netcat?” Last accessed July 11, 2014, <http://netcat.sourceforge.net/>.
- [14] *VirusTotal*. (June 17, 2014). “TSPY_DESLOC.AA.” Last accessed July 22, 2014, <https://www.virustotal.com/en/file/344a75c7a364f58bb62bb6bea30024c8ae9893b31d6706d213b5a93890fdce5c/analysis/>.

- [15] Maersk Menrige. (June 25, 2014). *TrendLabs Security Intelligence Blog*. “PlugX RAT with Time Bomb Abuses Dropbox for Command-and-Control Settings.” Last accessed July 16, 2014, <http://blog.trendmicro.com/trendlabs-security-intelligence/plugx-rat-with-time-bomb-abuses-dropbox-for-command-and-control-settings/>.
- [16] Nart Villeneuve and Jessa Dela Torre. (2013). *Trend Micro Security Intelligence*. “FAKEM RAT: Malware Disguised as Windows Messenger and Yahoo! Messenger.” Last accessed July 22, 2014, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-fakem-rat.pdf>.
- [17] Abraham Camba. (September 17, 2012). *TrendLabs Security Intelligence Blog*. “Unplugging PlugX Capabilities.” Last accessed July 22, 2014, <http://blog.trendmicro.com/trendlabs-security-intelligence/unplugging-plugx-capabilities/>.
- [18] Wikimedia Foundation Inc. (July 17, 2014). *Wikipedia*. “Transmission Control Protocol.” Last accessed July 16, 2014, http://en.wikipedia.org/wiki/Transmission_Control_Protocol.
- [19] Wikimedia Foundation Inc. (July 15, 2014). *Wikipedia*. “Protection Ring.” Last accessed July 17, 2014, http://en.wikipedia.org/wiki/Protection_ring.
- [20] Microsoft. (2014). *Windows Dev Center—Hardware*. “Packet Injection Functions.” Last accessed July 17, 2014, [http://msdn.microsoft.com/en-us/library/windows/hardware/ff569975\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/hardware/ff569975(v=vs.85).aspx).

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

©2014 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.



Securing Your Journey
to the Cloud

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.

Phone: +1.817.569,8900