

# US-CERT Technical Cyber Security Alert TA05-189A -- Targeted Trojan Email Attacks

*Source:* <http://www.derkeiler.com/Mailing-Lists/Cert/2005-07/0001.html>

---

*From:* US-CERT ([cert-advisory\\_at\\_cert.org](mailto:cert-advisory_at_cert.org))

*Date:* 07/08/05

Date: Fri, 8 Jul 2005 17:37:12 -0400

To: [cert-advisory@cert.org](mailto:cert-advisory@cert.org)

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Targeted Trojan Email Attacks

Original release date: July 08, 2005

Last revised: --

Source: US-CERT

Overview

The United States Computer Emergency Readiness Team (US-CERT) has received reports of an email based technique for spreading trojan horse programs. A trojan horse is an attack method by which malicious or harmful code is contained inside apparently harmless files. Once opened, the malicious code can collect unauthorized information that can be exploited for various purposes, or permit computers to be used surreptitiously for other malicious activity. The emails are sent to specific individuals rather than the random distributions associated with a phishing attack or other trojan activity. (Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that can be used for identity theft.) These attacks appear to target US information for exfiltration. This alert seeks to raise awareness of this kind of attack, highlight the important need for government and critical infrastructure systems owners and operators to take appropriate measures to protect their data, and provide guidance on proper protective measures.

Description

There are two distinct elements that make this attack technique significant. First, the trojans can elude conventional protective measures such as anti-virus software and firewalls, both key measures in protecting the US Critical Infrastructure networks. A number of

open source and tailored trojans, altered to avoid anti-virus detection, have been used. Trojan capabilities suggest that exfiltration of data is a fundamental goal. Second, the emails are sent to specific or targeted recipients. Unlike "phishing" attacks, the emails use social engineering to appear credible, with subject lines often referring to work or other subjects that the recipient would find relevant. The emails containing the trojanized attachments, or links to websites hosting trojanized files are spoofed, making it appear to come from a colleague or reliable party. The email attachments exploit known vulnerabilities to install a trojan on the user's computer. When opened, the file or link installs the trojan. Trojans can be configured to transmit information to a remote attacker using ports assigned to a common service (e.g., TCP port 80, which is assigned to Web traffic) and thereby defeat firewalls. Once the trojanized attachment is opened, a remote attacker can then perform the following functions:

- \* Collection of usernames and passwords for email accounts
- \* Collection of critical system information and scanning of network drives
- \* Use of infected machine to compromise other machines and networks
- \* Downloading of further programs (e.g., worms, more advanced trojans)
- \* Uploading of documents and data to a remote computer

US-CERT is working with other computer emergency response teams worldwide to address these types of attacks.

### Suggested Actions

Due to the targeted distribution of trojans spread in this way and the possibility of communication with remote attackers using ports assigned to common services, detection of this activity is problematic. US-CERT advises that system administrators take the following actions:

- \* Educate users to use an anti-virus scanner on all email attachments.
- \* Maintain and update anti-virus software and signatures to detect malware that may be associated with this attack.
- \* Block executable and/or suspect attachment types at email gateway or block the download of executable content via HTTP.
- \* Investigate anomalous slow-running machines, looking for unknown processes or unexpected Internet connections, as this may be an indication of malicious programs operating in the background. Encourage reporting and full investigation of such behavior.
- \* Update operating system and application software to patch vulnerabilities exploited in the past by these Trojans.
- \* Implement spam filtering to guard against infrastructures (e.g., dial-ups, open proxies and open relays) commonly used by the attackers.

- \* As Microsoft Office vulnerabilities have been targeted and exploited, ensure that Microsoft security bulletins are followed.

Microsoft Security Bulletins Search

<http://www.microsoft.com/technet/security/current.aspx>

- \* Turn off 'Preview Pane' functionality in email clients and set the default options to view opened emails as plain text
- \* Examine firewall logs of critical systems, or networks used for processing sensitive information, for connections to or from anomalous IP addresses.
- \* Consider traffic analysis to identify any compromised computers that are exfiltrating files. Data on the size and times of HTTP transactions or TCP port 80 flows may help detect exfiltration by highlighting connections where the data volume sent is far greater than that received from the remote server or when data is being sent at times outside of normal working hours.
- \* Analyze log files to determine whether the attackers are spoofing your domain.
- \* Consider implementing IP address lists of outbound Internet connections, denying access except from address ranges relevant to your business activities, such as a "default deny" policy. This provides some protection against computers in third countries being used by attackers to control trojans.

Incidents or suspected malicious activity of this nature, as well as all cyber security incidents affecting the US Critical Infrastructure should be reported to the United States Computer Emergency Readiness Team (US-CERT) via email to [soc@us-cert.gov](mailto:soc@us-cert.gov) or by telephone (703) 235-5110.

#### Vendor Product Names

The following anti-virus product names are associated with known trojans used in the attacks since January 2005.

#### McAfee

<<http://www.mcafee.com>>

- \* Backdoor-BCB
- \* BackDoor-CPY!chm
- \* Backdoor-TW
- \* Downloader-WY
- \* Exploit-1Table
- \* JS/BackDoor-CPY
- \* MultiDropper-MR
- \* Proxy-Sysgam
- \* Pusno
- \* StartPage-DH.dll

Sophos

<<http://www.sophos.com>>

- \* Troj/Agent-BX
- \* Troj/Agent-T
- \* Troj/DDrop-A
- \* Troj/Dloader-KF
- \* Troj/Dloader-KZ
- \* Troj/Lecna-C
- \* Troj/Nethief-M
- \* Troj/Nethief-N
- \* Troj/Nethief-O
- \* Troj/Netter-A
- \* Troj/Riler-E
- \* Troj/Riler-F
- \* Troj/Riler-J
- \* Troj/RPE-A
- \* Troj/Sharp-F
- \* Troj/VBDrop-A
- \* WM97/Loof-D

Symantec

<<http://www.symantec.com>>

- \* Trojan.Dropper
- \* Trojan.Mdropper.B
- \* Trojan.Riler.C

Trend Micro

<<http://www.trendmicro.com>>

- \* BKDR\_NETHIEF.L
- \* BKDR\_NETHIEF.R
- \* BKDR\_NETHIEF.S
- \* BKDR\_TUIMER.A
- \* TROJ\_AGENT.KZ
- \* TROJ\_SHARP.C
- \* TROJ\_WINBLUE.A
- \* W2KM\_PASSPRO.A
- \* W2KM\_PASSPRO.C
- \* W2KM\_PASSPRO.E

---

Feedback can be directed to US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov)

Produced 2005 by US-CERT, a government organization.

This document is available online.

<<http://www.us-cert.gov/cas/techalerts/TA05-189A.html>>

Cert: US-CERT Technical Cyber Security Alert TA05-189A -- Targeted Trojan Email Attacks

Terms of use

<<http://www.us-cert.gov/legal.html>>

Revision History

July 08, 2005: Initial release

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.1 (GNU/Linux)

iQEVawUBQs7q8hhoSezw4YfQAQJ2+Qf/X8cm1Z0+3NQoRNiyWxOz/0SR6uxsyQBO  
jd6jQpRwbuoFPQinnxJdf0kQLnIEqn9wcczn3ibjty8JjnZVMtjdq8PpTmkwy6jr  
H8l3Qm2J1hCgSgKQHweZLqdeKVvww2FGYRH12qHSKU++3NyZF+GZSoPgX/3QkM0D  
nxJ3sFnsysgt22SFcgL70MfD3nHocxIwLbnQfLvYWnFGci1fnS8sLng0Yj5UdKfu  
Bfa7ik4bmtRcL6r+tOweejI0dEqwbRgr/tHip55FqSrP15Ai6QXgrXpSMs1oYwLw  
geKcrxFSaKJh9gOj8IHSU5b+wLbvIgKpXou3PNs5cJxLM+ATw6eGRA==  
=TzGH

-----END PGP SIGNATURE-----