The Crimeware Landscape:
Malware, Phishing, Identity Theft and Beyond

A Joint Report of the US Department of Homeland Security – SRI International Identity Theft Technology Council and the Anti-Phishing Working Group.

October, 2006

Acknowledgments

This document was sponsored by the U.S. Department of Homeland Security Science and Technology Directorate (DHS S&T). Points of view expressed in this document are those of the author, and do not necessarily represent the official position of the DHS S&T Directorate.

Executive Summary

"Crimeware" is software that performs illegal actions unanticipated by a user running the software, which are intended to yield financial benefits to the distributor of the software.

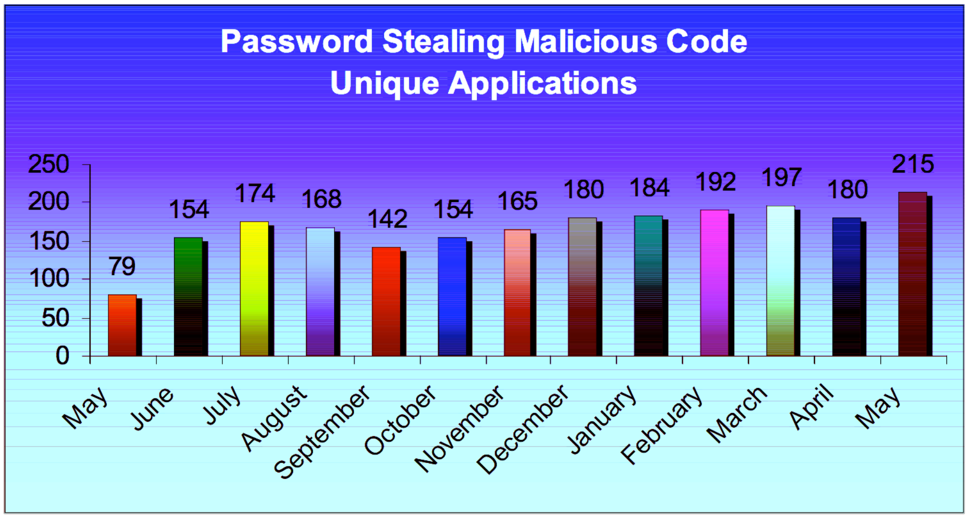
Crimeware is a ubiquitous fact of life in modern online interactions. It is distributed via many mechanisms, including:

- Social engineering attacks convincing users to open a malicious email attachment containing crimeware;
- Injection of crimeware into legitimate web sites via content injection attacks such as cross-site scripting;
- Exploiting security vulnerabilities through worms and other attacks on security flaws in operating systems, browsers, and other commonly installed software; and
- Insertion of crimeware into downloadable software that otherwise performs a desirable function.

Once installed, crimeware can be used for financial benefit by the attacker in many ways, including:

- Theft of personal information for fraudulent use and/or resale on a secondary market (as in a "phishing" attack);
- Theft of trade secrets and/or intellectual property, by commission, or for sale, blackmail or embarrassment;
- Distributed denial-of-service attacks launched in furtherance of online extortion schemes;
- Spam transmission;
- "Click fraud" that generates revenues by simulating traffic to online advertisements;
- "Ransomware" that encrypts data and extorts money from the target to restore it; and
- Use of consolidated personal information for furtherance of additional attacks, such as obtaining contact lists and email addresses to additionally or more precisely target the victim and his or her associates.

Crimeware implementations and deployments are an increasingly serious problem. In the month of May 2006, at least 215 unique keyloggers – just one type of crimeware – were observed in the wild.



Keylogger Programs in the Wild, Unique Signatures (2005-06)

Source: Websense/APWG

This report presents a taxonomy of crimeware, with an emphasis on the theft of sensitive information, discusses how it is installed and what it does, and delineates opportunities to deploy countermeasures.

Table of Contents

Introduction

Online identity theft, in which confidential information is illicitly obtained through a computer network and used for profit, is a rapidly growing enterprise. Credible estimates of the direct financial losses due to “phishing” alone exceed a billion dollars per year. Indirect losses are much higher, including customer service expenses, account replacement costs, and higher expenses due to decreased use of online services in the face of widespread fear about the security of online financial transactions.

Increasingly, online identity theft is perpetrated using malicious software known as *crimeware*. Crimeware can be used to obtain many kinds of confidential information, including user names and passwords, social security numbers, credit card numbers, bank account numbers, and personal information such as birthdates and mothers’ maiden names.

In addition to online identity theft, crimeware is used in targeted attacks against institutions, such as theft of access credentials to corporate VPNs and theft of intellectual property or business data. Crimeware can also be used in distributed denial-of-service attacks, which are used to extort money from businesses, and in “click fraud” in which online advertisers are cheated into paying criminals who simulate clicks on advertisements they host themselves. Instances of “ransomware” have also occurred in which data on a compromised machine is encrypted, and an offer is made to decrypt the data for a fee.

Crimeware is a subclass of the more general category of *malware*, which refers generally to unwanted software running on a user’s computer that performs malicious actions. In addition to crimeware, malware encompasses legal but malicious software such as adware and spyware, and illegal software without a commercial purpose, such as destructive viruses.

This report is concerned primarily with crimeware that is used in the theft of identity-related credentials and other sensitive data, rather than crimeware that is used in extortion rings or other online criminal activity. Malware that is not crimeware is outside the scope of this report, though it may be incidentally discussed with reference to technologies shared between crimeware and other types of malware.

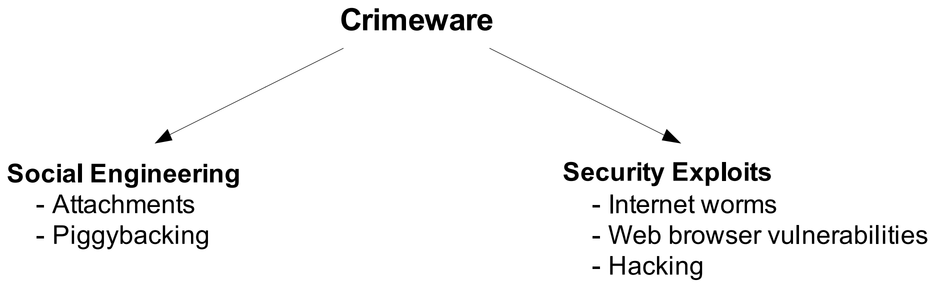


Figure 1. Crimeware Propagation Techniques

As shown in figure 1, crimeware is generally spread either by social engineering or by exploiting a security vulnerability.

A typical social engineering attack is to convince a user to open an email attachment or download a file from a web site, often claiming the attachment has something to do with pornography, salacious celebrity photos or gossip. Some downloadable software, such games or video player "accelerators," can also contain malware.

Malware is also spread by exploits of security vulnerabilities, either by propagating a worm or virus that takes advantage of a security vulnerability to install the malware, or by making the malware available on a web site that exploits a security vulnerability. Traffic may be driven to a malicious web site via social engineering such as spam messages promising some appealing content at the site, or by injecting malicious content into a legitimate web site by exploiting a security weakness such as a cross-site scripting vulnerability on the site.

Crimeware attacks often span multiple countries, and are commonly perpetrated by organized criminals. This report describes and categorizes various types of crimeware and discusses the structural elements common to various attacks.

Prevalence of Crimeware

Information theft via crimeware is a rapidly increasing problem. Phishing scams are increasingly being performed via crimeware, as the observed growth of keylogger-specific crimeware during 2005 and 2006 shown in figure 2 indicates.

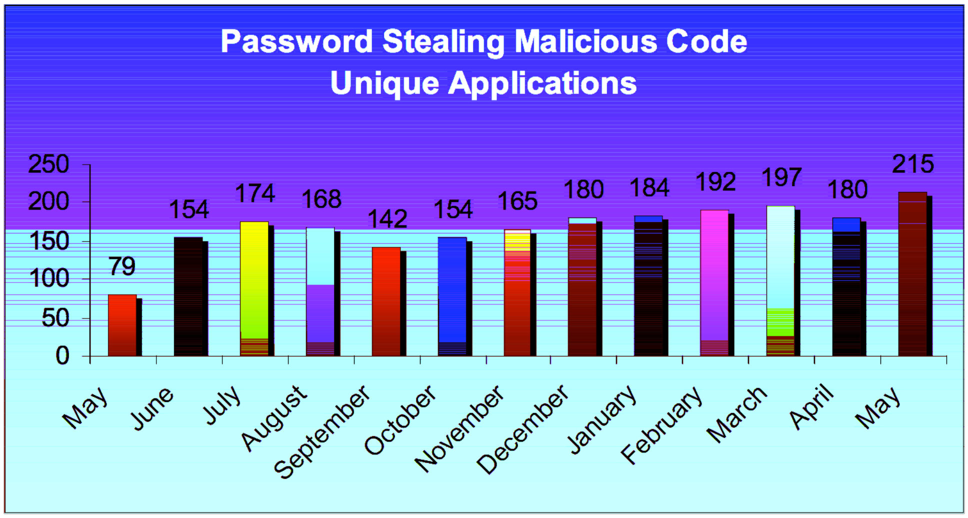


Figure 2. Keylogger Programs in the Wild, Unique Signatures (2005-06)

Source: Websense/APWG

The number of sites distributing such crimeware is growing even more rapidly, as shown in figure 3. This trend reflects the growing commoditization of crimeware technology and the use of multiple hosts, such as botnets, for distribution and data collection. The use of more web sites per attack makes it more difficult to shut down malicious web sites to stem the spread and impact of crimeware.

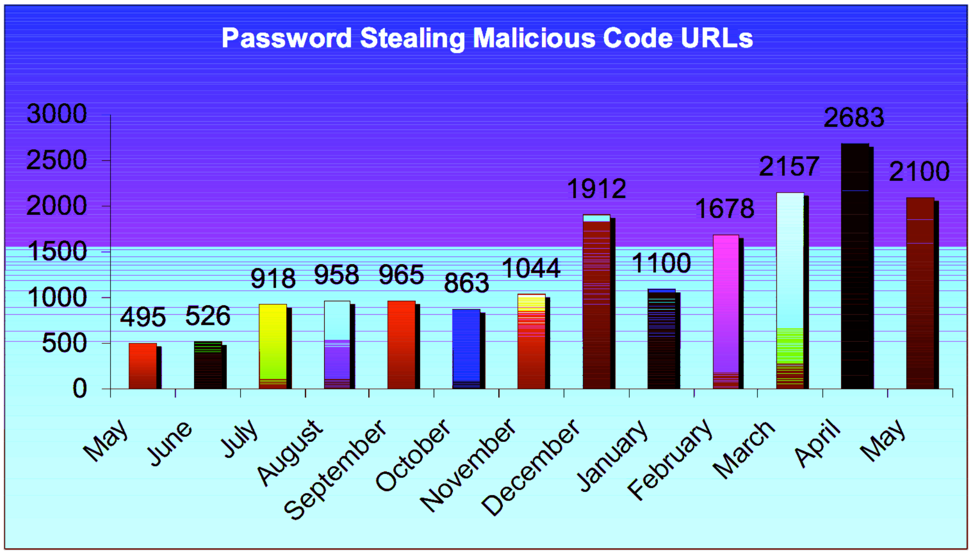


Figure 3. Keylogger Distribution Sites (2005-06)

Source: Websense/APWG

Crimeware Threat Model and Taxonomy

Crimeware comes in many different flavors. Cybercriminals are technically innovative, and can afford to invest in technology. The most dangerous crimeware attacks are carried out as professional organized crime. As financial institutions have increased their online presence, the economic value of compromising account information has increased dramatically. Cybercriminals such as phishers can afford an investment in technology commensurate with the illegal benefits gained by their crimes.

Given the rapid evolution of cybercrime, a comprehensive catalogue of crimeware technologies is not feasible. Several types of crimeware are discussed below, as representative of the species. The distinctions between crimeware variants are porous, as many attacks are hybrids that employ multiple technologies. For example, a deceptive phishing email could direct a user to a site that has been compromised with content injection, which installs a backdoor on the victim's computer via a browser security vulnerability. This backdoor is then used to install crimeware that poisons the user's hosts file and enables a pharming attack. Subsequent attempts to reach legitimate web sites will be rerouted to phishing sites, where confidential information is compromised using a man-in-the-middle attack. At the same time, other malicious software can also be installed using the backdoor, such as a mail relay to transmit spam and a remotely controlled slave that listens over a chat channel and participates in a distributed denial of service attack when a command to do so is received.

Notwithstanding the proliferation of various types of crimeware, a crimeware attack on a conventional computing platform without protected data or software can be roughly diagrammed as shown in figure 4.

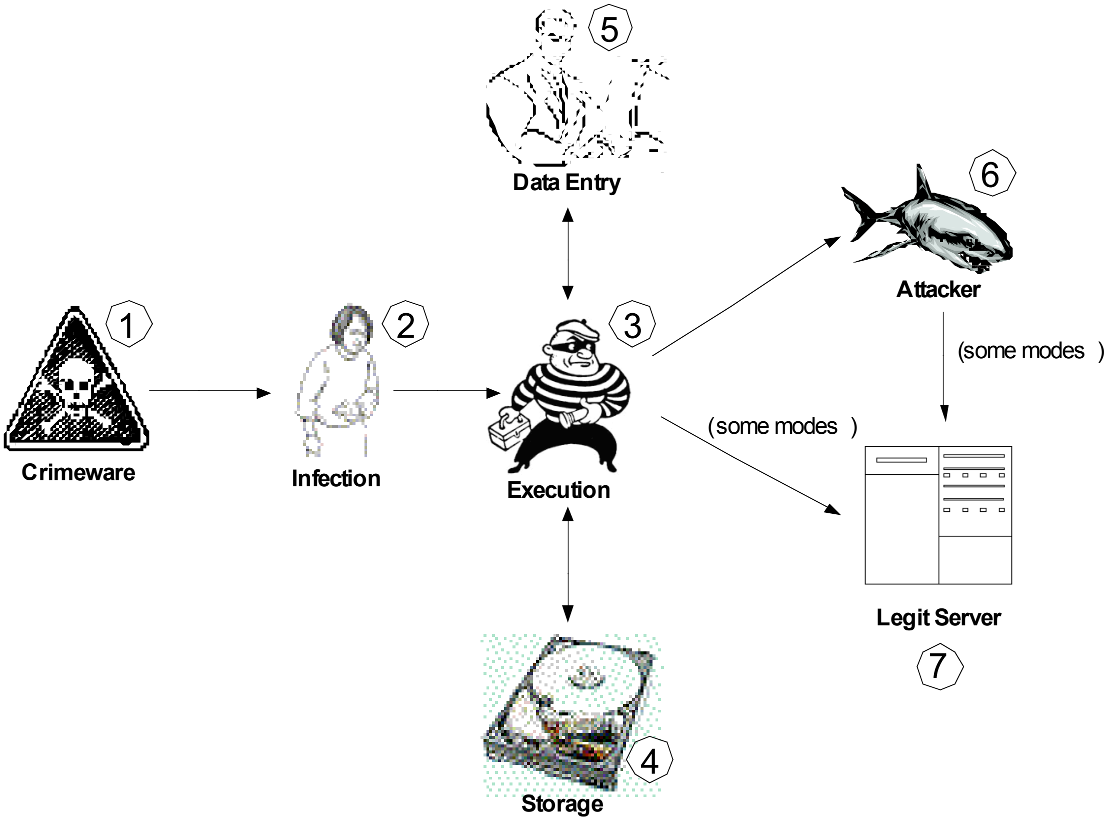


Figure 4. Anatomy of a Crimeware Attack

In this diagram, the stages of a crimeware attack are categorized as follows:

1. *Crimeware is distributed*. Depending on the particular crimeware attack, crimeware may be distributed via social engineering (as is the case in malicious email attachments and piggyback attacks) or via an exploit of a security vulnerability (as is the case in web browser security exploits, internet worms, and hacking).
2. *The computing platform is infected*. Infection takes many forms, which are discussed separately below. In some cases, the crimeware itself is ephemeral and there may be no executable "infection" stage, as in immediate data theft or system reconfiguration attacks. In such cases, an attack leaves behind no persistent executable code.
3. *The crimeware executes*, either as part of a one-time attack such as data theft or system reconfiguration, as a background component of an attack such as a rootkit, or by invocation of an infected component.
4. *Confidential data is retrieved from storage*, in attacks such as data theft.
5. *Confidential information is provided by the user*, in attacks such as keyloggers and web Trojans.

6. *The attacker misappropriates confidential data*. Data may come from any of several sources depending on the type of crimeware involved, as discussed above.
7. *The legitimate server receives confidential data*, either from the executing crimeware (in attacks in which data is explicitly compromised by the crimeware) or from the attacker (in man-in-the-middle attacks).

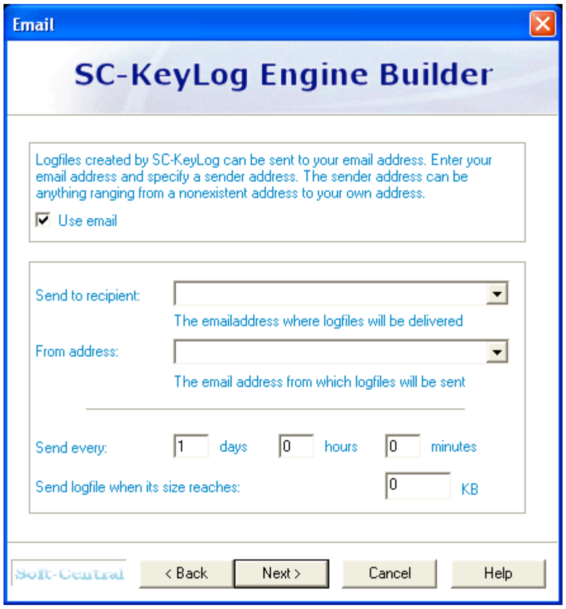
A Crimeware Menagerie

Many varieties of crimeware are explored below, all of which follow the stages outlined above. Crimeware species include keyloggers and screenloggers, redirectors, session hijackers, web Trojans, transaction generators, system reconfigurators and data stealers. In addition, crimeware based on man-in-the-middle attacks is examined, and rootkits that can prevent detection of foreign code are discussed.

Keyloggers and Screenloggers

Keyloggers are programs that install themselves either into a web browser or as a device driver, which monitor data being input and send relevant data to a phishing server. Keyloggers use a number of different technologies, and may be implemented in many ways, including:

- A browser helper object that detects changes to the URL and logs information when a URL is affiliated with a designated credential collection site;
- A device driver that stores keyboard and mouse inputs in conjunction with monitoring the user’s activities; and
- A *screenlogger* that monitors both the user’s inputs and portions of the display, to thwart alternate on-screen input security measures.



Logfiles created by SC-KeyLog can be sent to your email address. Enter your email address and specify a sender address. The sender address can be anything ranging from a nonexistent address to your own address.

☑ Use email

Send to recipient:
The emailaddress where logfiles will be delivered

From address:
The email address from which logfiles will be sent

Send every: 1 days 0 hours 0 minutes

Send logfile when its size reaches: 0 KB

Figure 5. Keylogger Configurator

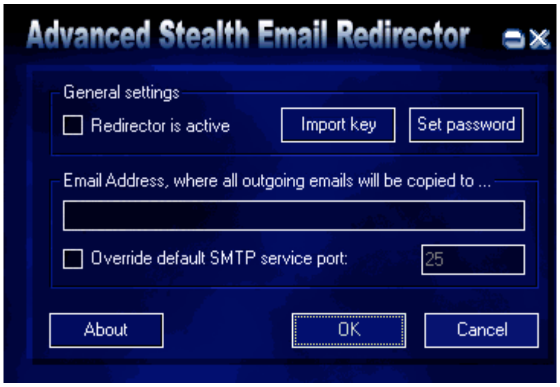
Keyloggers may collect credentials for a wide variety of sites. As with many crimeware varieties, configurators are available to automate construction of customized keyloggers (as shown in figure 5). Keyloggers are often packaged to monitor the user's location, and to transmit only credentials associated with particular sites back to the attacker. Often, hundreds of such sites are targeted, including financial institutions, information portals, and corporate VPNs. Various secondary damage can be caused after a keylogger compromise. In one real-world example, a credit reporting agency was targeted by a keylogger spread via pornography spam. This led to the compromise of over 50 accounts with access to the agency, which in turn were used to compromise as many as 310,000 sets of personal information from the credit reporting agency's database.

Email and Instant Messaging Redirectors

Email redirectors are programs that intercept and relay outgoing emails, and send an additional copy to an unintended address to which an attacker has access.

Instant messaging redirectors monitor instant messaging applications and transmit transcripts to an attacker.

Email and instant messaging redirectors, examples of which are shown in figures 6 and 7, are used for corporate espionage as well as personal surveillance.


Advanced Stealth Email Redirector

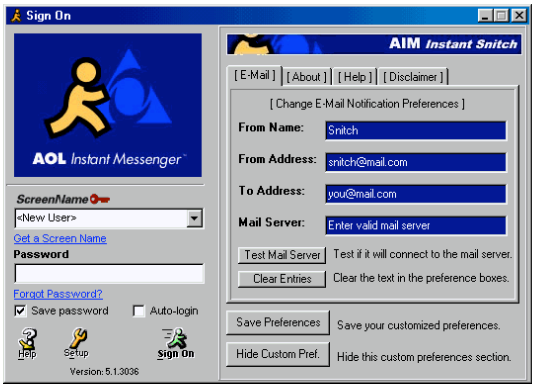
General settings

□ Redirector is active

Email Address, where all outgoing emails will be copied to ...

□ Override default SMTP service port: 25

Figure 6. Email Redirector


Sign On

ScreenName <New User>

Password

☑ Save password

□ Auto-login

Version: 5.1.3036

AIM Instant Snitch

[Change E-Mail Notification Preferences]

From Name: Snitch

From Address: snitch@mail.com

To Address: you@mail.com

Mail Server: Enter valid mail server

Test Mail Server — Test if it will connect to the mail server.

Clear Entries — Clear the text in the preference boxes.

Save Preferences — Save your customized preferences.

Hide Custom Pref. — Hide this custom preferences section.

Figure 7. Instant Messaging Redirector

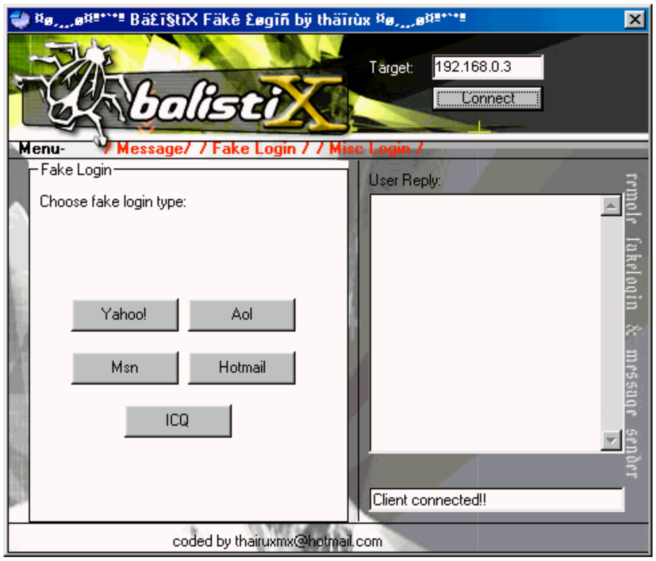
Session Hijackers

Session hijacking refers to an attack in which a legitimate user session is commandeered. In a session hijacking attack, a user's activities are monitored, typically by a malicious browser component. When the user logs into his or her account, or initiates a transaction, the malicious software "hijacks" the session to perform malicious actions, such as transferring money, once the user has legitimately established his or her credentials.

Session hijacking can be performed on a user's local computer by malware, or can also be performed remotely as part of a man-in-the-middle attack, which is discussed separately below. When performed locally by malware, session hijacking can look to the targeted site exactly like a legitimate user interaction, being initiated from the user's home computer.

Web Trojans

Web Trojans are malicious programs that pop up over login screens to collect credentials. The user believes that he or she is entering information on a web site, while in fact the information is being entered locally, then transmitted to the attacker for misuse.


¤ø,¸¸,ø¤º°`°º¤ Bä£ï§tïX Fäkê £øgïñ bÿ thäïrùx ¤ø,¸¸,ø¤º°`°º¤
balistiX
Connect
Menu-
/ Message/ / Fake Login / / Misc Login /
Fake Login
Yahoo!
Aol
Msn
Hotmail
ICQ
User Reply:
remote fakelogin & message sender

Target: 192.168.0.3

Choose fake login type:

Client connected!!

coded by thairuxmx@hotmail.com

Figure 8. Web Trojan Configurator

Transaction Generators

Unlike many of the other types of crimeware discussed in this report, a transaction generator is targeted not at an end-user's computer but at a computer inside a transaction processing center such as a credit card processor.

A transaction generator generates fraudulent transactions for the benefit of the attacker, from within the payment processor. Transaction generators often additionally intercept and compromise credit card data.

Transaction generators are typically installed by hackers who have targeted the transaction processing center and compromised its security.

System Reconfiguration Attacks

System reconfiguration attacks, such as hostname lookup attacks and proxy attacks, modify settings on a user's computer to cause information to be compromised.

Hostname Lookup Attacks

When establishing a connection with a remote computer such as a web server belonging to a bank or other target, a hostname lookup is normally performed to translate a domain name such as “bank.com” to a numeric IP address such as 198.81.129.100. Hostname lookup attacks interfere with the integrity of the lookup process for a domain name. Hostname lookup attacks are commonly called “pharming.”

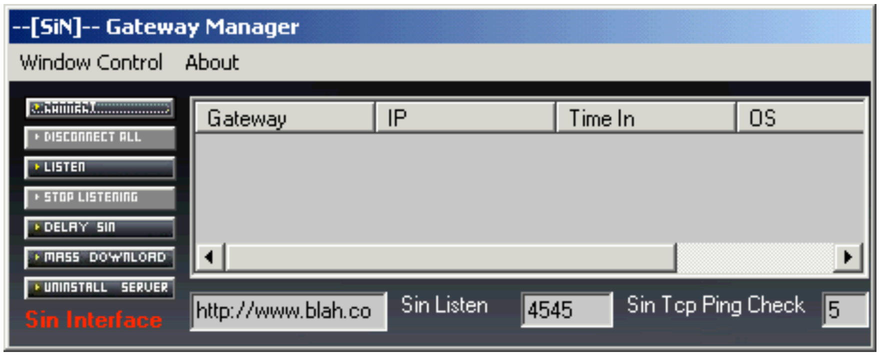
One form of hostname lookup attack is to interfere with the Domain Name System (DNS), for example by hacking a DNS server. However, hostname lookup attacks are more commonly performed locally by crimeware that modifies the *hosts file* on the victim's computer. A hosts file is used by a computer to see whether a domain or host name is known to the local machine with a predetermined address, before consulting DNS. If the domain or host name appears in the hosts file, the corresponding address will be used, without regard to what a DNS query for that domain might return. If this file is modified, then “www.bank.com” can be made to refer to a malicious address. When the user goes there, he or she will see a legitimate-looking site and enter confidential information, which actually goes to the attacker.

Another way to interfere with hostname lookups is to alter the system configuration of a victim’s computer to change the DNS server to a malicious server controlled by the attacker. When a user navigates to a correctly named site, such a server can send the user to a fraudulent site where confidential information is collected.

Another form of hostname lookup attack involves polluting the user’s DNS cache with incorrect information that will be used to direct the user to an incorrect location. If the user has a misconfigured DNS cache, this can be done by simply providing incorrect information. It can also be accomplished by hacking a legitimate DNS server, or by polluting the cache of a misconfigured legitimate DNS server. Such attacks do not fall within the definition of crimeware, as they do not involve software that runs on the victim’s computer.

Proxy Attack

Another type of system reconfiguration attack is to install a proxy through which the user’s network traffic will be passed. The attacker can glean confidential information from the traffic while retransmitting it back and forth between the victim and a remote web site. This is a form of a man-in-the-middle attack, which is discussed separately.



Gateway	IP	Time In	OS

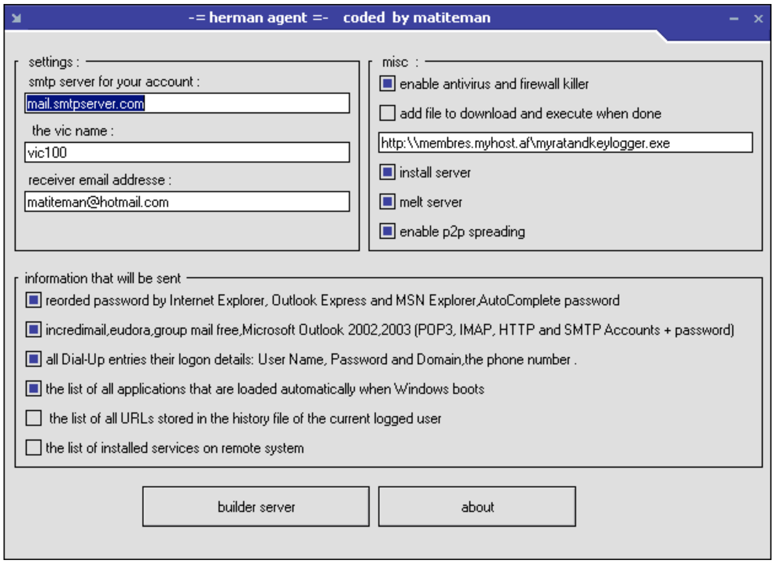
http://www.blah.co Sin Listen 4545 Sin Tcp Ping Check 5

Figure 9. TCP/IP Proxy Manager

Proxies come in many types, including HTTP proxies, TCP/IP drivers, and browser helper objects that proxy web traffic from the browser. Many are manageable using a remote interface, such as the one shown in figure 9.

Data Theft

Once malicious code is running on a user’s machine, it can directly steal confidential data stored on the computer. Such data can include passwords, activation keys to software, sensitive correspondence, and any other information that is stored on a victim’s computer. Some confidential data, such as passwords stored in browser and email clients, is accessible in standard locations. By automatically filtering data looking for information that fits patterns such as a social security number, a great deal of other sensitive information can also be obtained.



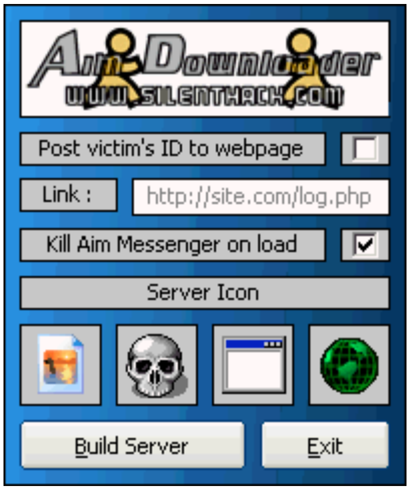
settings :
smtp server for your account : mail.smtpserver.com
the vic name : vic100
receiver email addresse : matiteman@hotmail.com

misc :
☑ enable antivirus and firewall killer
□ add file to download and execute when done
http:\\membres.myhost.af\myratandkeylogger.exe
☑ install server
☑ melt server
☑ enable p2p spreading

information that will be sent
☑ reorded password by Internet Explorer, Outlook Express and MSN Explorer,AutoComplete password
☑ incredimail,eudora,group mail free,Microsoft Outlook 2002,2003 (POP3, IMAP, HTTP and SMTP Accounts + password)
☑ all Dial-Up entries their logon details: User Name, Password and Domain,the phone number .
☑ the list of all applications that are loaded automatically when Windows boots
□ the list of all URLs stored in the history file of the current logged user
□ the list of installed services on remote system

Figure 10. Data Theft Configuration Screen (files in standard locations)

Data theft is also commonly performed by crimeware performing corporate (or possibly governmental) espionage, using software such as that shown in figures 10 and 11. High-value machines can be targeted, but some such espionage can also be based on large-scale attacks, because personal computers often contain the same confidential information that is also stored on better-protected enterprise computers. In addition to espionage for hire, confidential memos or design documents can be publicly leaked, causing economic damage or embarrassment.



Post victim's ID to webpage □
Link : http://site.com/log.php
Kill Aim Messenger on load ☑
Server Icon

Figure 11. Data Theft Configuration Screen (arbitrary file theft via AIM)

Man-in-the-Middle Attacks

A man-in-the-middle attack, schematically illustrated in figure 12, refers generally to an attack in which the attacker positions himself between two communicating parties and gleans information to which he should not have access. Messages intended for the legitimate site are passed to the attacker instead, who saves valuable information, passes the messages to the legitimate site, and forwards the responses back to the user.

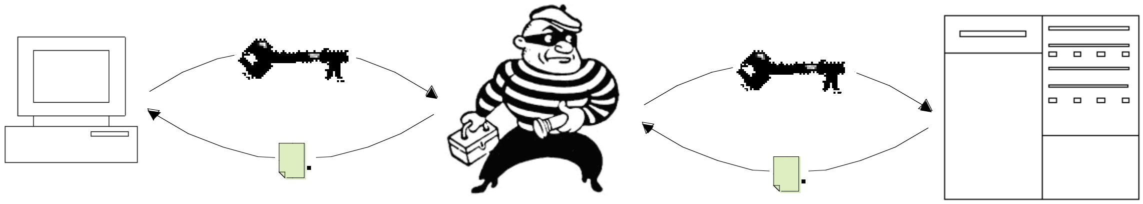


Figure 12. Man-in-the-Middle Attack

Examples of a man-in-the-middle attack in the context of crimeware-based information theft include:

- A session hijacking attack, in which information is received from a user and passed through to the legitimate site until the desired authentication and/or transaction initiation has been performed, whereupon the session is hijacked;
- A hostname lookup ("pharming") attack, in which a web site at the expected host name, but with the wrong IP address, relays data from the user to the legitimate site and vice-versa, to provide verisimilitude and delay detection; and
- A web proxy attack, in which a malicious web proxy receives all web traffic from a compromised computer and relays it to a legitimate site, collecting credentials and other confidential information in the process.

Man-in-the-middle attacks are difficult for a user to detect, because a legitimate site can appear to work properly, and there may be no external indication that anything is wrong.

Normally, SSL web traffic will not be vulnerable to a man in the middle attack. The handshake used by SSL ensures that the session is established with the party named in the server’s certificate, and that an external attacker cannot obtain the session key; and SSL traffic is encrypted using the session key so it cannot be decoded by an eavesdropper. Proxies normally have provisions for tunneling such encrypted traffic without being able to access its contents. However, browsers and other standard software applications generally silently accept cryptographic certificates from trusted certificate authorities, and crimeware can modify a system configuration to install a new trusted certificate authority. Having done so, a proxying intermediary can create its own certificates in the name of any SSL-protected site. These certificates, since they are coming from a “trusted” certificate authority due to the system reconfiguration, will be unconditionally accepted by the local software. The intermediary is therefore able to decrypt the traffic and extract confidential information, and re-encrypt the traffic to communicate with the other side. In practice, however, most man-in-the-middle attacks simply do not use SSL, since users do not generally check for its presence.

Man-in-the-middle attacks can compromise authentication credentials other than passwords, such as one-time or time-varying passcodes generated by hardware devices. Such stolen credentials can be used by an attacker for authentication as long as they remain valid.

Rootkits

A rootkit refers generally to any software that hides the presence and activity of malicious software. Rootkits can be as simple as crude replacements of administrative software that is commonly used to monitor running processes on a computer, or as complex as sophisticated kernel-level patches that enforce invisibility of protected malicious code, even to detectors with access to kernel-level data structures.

It has often been proposed that computers can be protected from malware by running them in a virtual machine. In an inversion of this scheme, it is also possible for a rootkit to virtualize the operating system and applications of a host computer, rendering detection of crimeware, which runs outside of the virtual machine, extremely difficult from within the virtual machine. This attack can be aided by modern processor features supporting virtualization.

It is also theoretically possible for crimeware to install itself not only in the memory and hard drive of an infected computer, but even in nonvolatile storage of its hardware devices, such as an ACPI BIOS or a graphics card. Such exploits have been proven possible in laboratory experiments, but have yet to appear in the wild.

Crimeware Distribution

Crimeware is distributed in many ways. The various distribution models include distribution leveraging social engineering (attachment, piggybacking), exploit-based distribution via server (web browser exploit, including content injection), exploit-based distribution via infected computer (internet worms), and distribution via human (hacking). Distribution of crimeware may blur these distinctions, such as a social engineering “phishing” attack that directs users to a web site that installs crimeware via a web browser exploit.

Distribution via Attachment

In this mode of distribution, crimeware is sent as an email or instant message attachment. A user is tricked into opening the attachment because it appears to have some value, either salacious (e.g. scandalous pictures or video) or practical (e.g. a security scanning “update” or a video codec “accelerator”).

Another form of attachment-based distribution is to distribute crimeware by embedding it in an attractive device such as a USB drive that is “lost” near a target such as a corporation being targeted for corporate espionage. The finders of such devices often attach them to their computers, which can cause software to execute automatically, or may even install their contents out of curiosity.

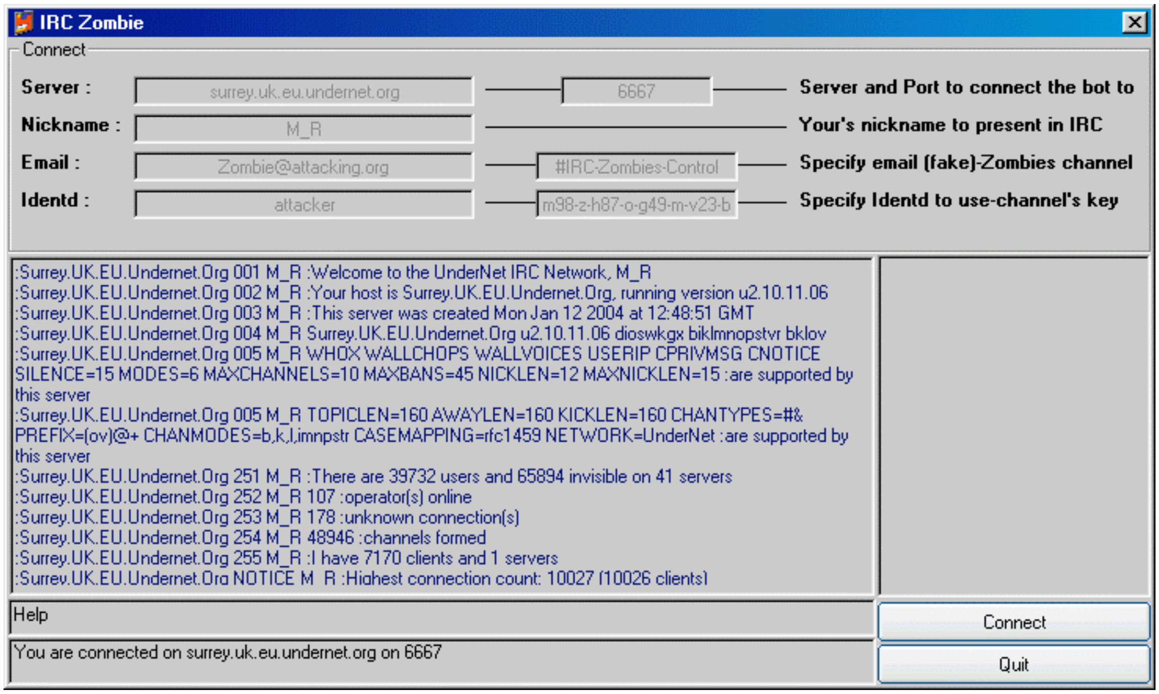
Distribution via Piggybacking

Crimeware can also be distributed within an application that is being downloaded for another purpose. For example, legitimate applications can be infused with malicious functionality, or applications claiming to perform a useful function – or actually performing a useful function – can have malicious code embedded within them. This is a common mode of propagation for software that pops up advertising (“adware” and “spyware”). In some cases, malicious software can be installed with a user’s ostensible consent, by obtaining permission through the use of lengthy and confusing end-user license agreements that make it very difficult to understand what is being authorized.

Distribution via Internet Worm

Crimeware can be spread by internet “worms” that exploit security vulnerabilities. An infected machine will typically scan to find other vulnerable machines, and infect them as well.

Worms usually install a backdoor on infected computers, which allows an attacker (either the worm author or an independent or affiliated attacker) to subsequently install crimeware on computers. Infected computers are frequently recruited into a botnet that is controlled by the attacker, typically via an IRC channel or similar means. An example of software for controlling a botnet is shown in figure 13.



Server : surrey.uk.eu.undernet.org 6667 Server and Port to connect the bot to

Nickname : M_R Your's nickname to present in IRC

Email : Zombie@attacking.org #IRC-Zombies-Control Specify email (fake)-Zombies channel

Identd : attacker m98-z-h87-o-g49-m-v23-b Specify Identd to use-channel's key

```
:Surrey.UK.EU.Undernet.Org 001 M_R :Welcome to the UnderNet IRC Network, M_R
:Surrey.UK.EU.Undernet.Org 002 M_R :Your host is Surrey.UK.EU.Undernet.Org, running version u2.10.11.06
:Surrey.UK.EU.Undernet.Org 003 M_R :This server was created Mon Jan 12 2004 at 12:48:51 GMT
:Surrey.UK.EU.Undernet.Org 004 M_R Surrey.UK.EU.Undernet.Org u2.10.11.06 dioswkgx biklmnopstvr bklov
:Surrey.UK.EU.Undernet.Org 005 M_R WHOX WALLCHOPS WALLVOICES USERIP CPRIVMSG CNOTICE
SILENCE=15 MODES=6 MAXCHANNELS=10 MAXBANS=45 NICKLEN=12 MAXNICKLEN=15 :are supported by
this server
:Surrey.UK.EU.Undernet.Org 005 M_R TOPICLEN=160 AWAYLEN=160 KICKLEN=160 CHANTYPES=#&
PREFIX=(ov)@+ CHANMODES=b,k,l,imnpstr CASEMAPPING=rfc1459 NETWORK=UnderNet :are supported by
this server
:Surrey.UK.EU.Undernet.Org 251 M_R :There are 39732 users and 65894 invisible on 41 servers
:Surrey.UK.EU.Undernet.Org 252 M_R 107 :operator(s) online
:Surrey.UK.EU.Undernet.Org 253 M_R 178 :unknown connection(s)
:Surrey.UK.EU.Undernet.Org 254 M_R 48946 :channels formed
:Surrey.UK.EU.Undernet.Org 255 M_R :I have 7170 clients and 1 servers
:Surrey.UK.EU.Undernet.Org NOTICE M_R :Highest connection count: 10027 (10026 clients)
```

Help

You are connected on surrey.uk.eu.undernet.org on 6667

Figure 13. Botnet Controller

Crimeware installed through backdoors often includes keyloggers, phishing data collectors, and mail relays used for sending spam.

Distribution via Web Browser Exploit

Web browsers are complex applications, and contain many security vulnerabilities. Such vulnerabilities are a common distribution vector for crimeware.

When a user visits a malicious web site, a vulnerability is exploited by code on the site. Such vulnerabilities can involve scripting, parsing, processing and displaying content, or any other component that can cause the browser to execute malicious code.

Not all web browser exploits are disseminated via malicious web sites. A legitimate web site can also distribute a crimeware payload, via a content injection attack such as cross-site scripting.

Content Injection Attacks

Content injection refers to inserting malicious content into a legitimate site. In addition to deceptive actions such as redirecting to other sites, malicious content can install crimeware on a user's computer through a web browser vulnerability or by social engineering, such as asking a user to download and install anti-virus software that actually contains crimeware.

There are three primary classes of content injection attacks, each of which has many possible variations:

- Hackers can compromise a server through a security vulnerability and replace or augment the legitimate content with malicious content.
- Crimeware can be inserted into a site through a cross-site scripting vulnerability. A cross-site scripting vulnerability is a programming flaw involving content coming from an external source, such as a blog, a user review of a product on an e-commerce site, an auction, a message in a discussion board, a search term, or a web-based email. Such externally supplied content can be a malicious script or other content that is not properly filtered out by software on the site's server, and runs in the web browser of a visitor to the site.
- Malicious actions can be performed on a site through a SQL injection vulnerability. This is a way to cause database commands to be executed on a remote server. Such command execution can cause information leakage, provide a vector for vandalism, or enable injection of malicious content that will subsequently be transmitted to a victim. Like cross-site scripting vulnerabilities, SQL injection vulnerabilities are a result of improper filtering.

Cross-site scripting and SQL injection are propagated through two different primary vectors. In one vector, malicious content is injected into data stored on a legitimate web server, which a victim is exposed to. In the other vector, malicious content is embedded into a URL that the user visits when he or she clicks on a link. This is commonly a URL that includes components that will be displayed on screen or used as part of a database query, such as an argument to a search function.

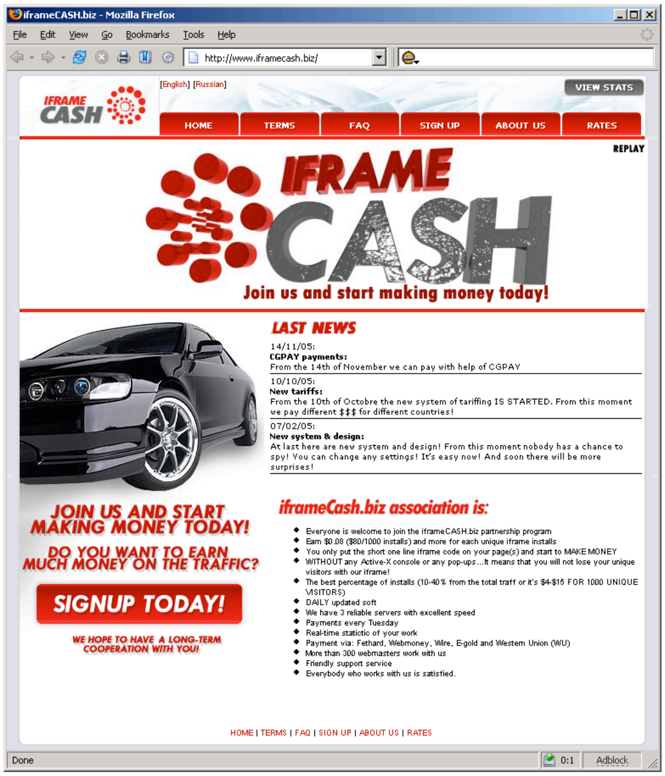
Distribution via Hacking

Crimeware can be installed by manually exploiting a security vulnerability or misconfiguration, i.e. by hacking into a system. This is generally infeasible for large-scale crimeware attacks, but can be effective against specific targets, such as corporate espionage or installation of transaction generators. Hacking sometimes plays a role in phishing attacks, in which hackers manually compromise a DNS server and configure it to direct DNS queries for targeted domains to phishing servers, or in which legitimate sites are hacked and malicious content is placed on them.

Manual hacking was once the purview of skilled hackers. However the availability of prepackaged port scanners and other hacking tools have enabled a generation of "script kiddies," who frequently lack the requisite knowledge to find new exploits, but can run hacking-aiding software that performs the more complex technical functions required to identify and exploit known vulnerabilities.

Distribution via Affiliate Marketing

Several affiliate marketing programs, such as the one shown in figure 14, have sprung up that offer financial rewards for web site operators to install malware on users' computers via security vulnerabilities. While the majority of such programs install adware and spyware, crimeware is now also being propagated through such affiliate networks. Parties that install malicious software on visitors' computers are compensated with payments typically ranging from 8 to 50 cents per installation, depending on the country in which the visitor is located.


iframeCASH.biz - Mozilla Firefox
File
Edit
View
Go
Bookmarks
Tools
Help
http://www.iframecash.biz/
[English] [Russian]
IFRAME CASH
VIEW STATS
HOME
TERMS
FAQ
SIGN UP
ABOUT US
RATES
REPLAY
IFRAME CASH
Join us and start making money today!
JOIN US AND START MAKING MONEY TODAY!
DO YOU WANT TO EARN MUCH MONEY ON THE TRAFFIC?
SIGNUP TODAY!
WE HOPE TO HAVE A LONG-TERM COOPERATION WITH YOU!
HOME | TERMS | FAQ | SIGN UP | ABOUT US | RATES
Done
0:1
Adblock

LAST NEWS

14/11/05:
CGPAY payments:
From the 14th of November we can pay with help of CGPAY

10/10/05:
New tariffs:
From the 10th of Octobre the new system of tariffing IS STARTED. From this moment we pay different $$$ for different countries!

07/02/05:
New system & design:
At last here are new system and design! From this moment nobody has a chance to spy! You can change any settings! It's easy now! And soon there will be more surprises!

iframeCash.biz association is:

- Everyone is welcome to join the iframeCASH.biz partnership program
- Earn $0.08 ($80/1000 installs) and more for each unique iframe installs
- You only put the short one line iframe code on your page(s) and start to MAKE MONEY
- WITHOUT any Active-X console or any pop-ups...It means that you will not lose your unique visitors with our iframe!
- The best percentage of installs (10-40% from the total traff or it's $4-$15 FOR 1000 UNIQUE VISITORS)
- DAILY updated soft
- We have 3 reliable servers with excellent speed
- Payments every Tuesday
- Real-time statictic of your work
- Payment via: Fethard, Webmoney, Wire, E-gold and Western Union (WU)
- More than 300 webmasters work with us
- Friendly support service
- Everybody who works with us is satisfied.

Figure 14. Crimeware Affiliate Program Site

Crimeware Information Compromise Points

Various types of crimeware have been identified that compromise information at different points in the overall crimeware attack shown in figure 4, reproduced below. Each type of crimeware has an *infection point*, at which the system state is altered (either permanently or ephemerally) to include malicious code or poisoned data, and a *data compromise point*, at which sensitive information is actually obtained by an attacker.

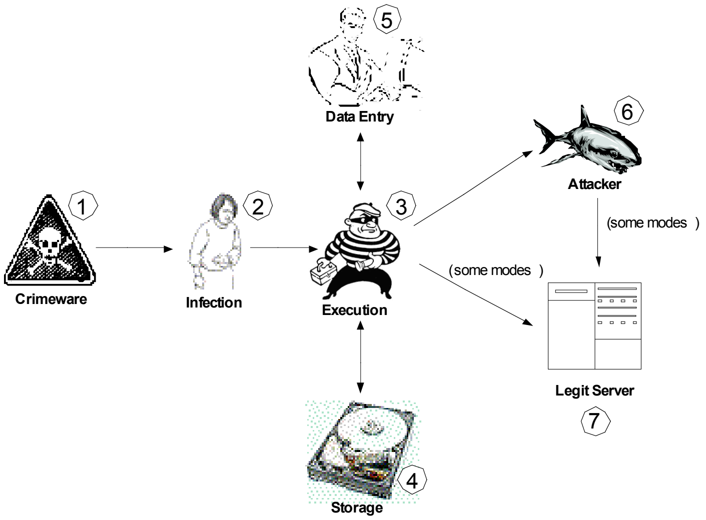


Figure 4 (repeated). Anatomy of a Crimeware Attack

According to the steps shown in figure 4, the infection and data compromise points in each of the types of crimeware enumerated in this report are as follows:

Attack Type	**Infection Point**	**Data Compromise Point**
Keylogger/Screenlogger	2	5 (I/O device)
Email/IM Redirector	2	6 (network)
Session Hijacker	2	6 (network)
Web Trojan	2	5 (I/O device)
Transaction Generator	2	N/A
System Reconfiguration Hostname Lookup Proxy	 3 (execution) 3 (execution)	 5 (web form) 6 (network)
Data Theft	3 (execution - ephemeral)	4 (storage)

Crimeware Chokepoints and Countermeasures

The infection point and the data compromise point are the primary chokepoints at which a countermeasure may be applied to each class of crimeware. Any other steps followed by a particular example of malware prior to the data compromise are potential secondary chokepoints at which a countermeasure may be applied.

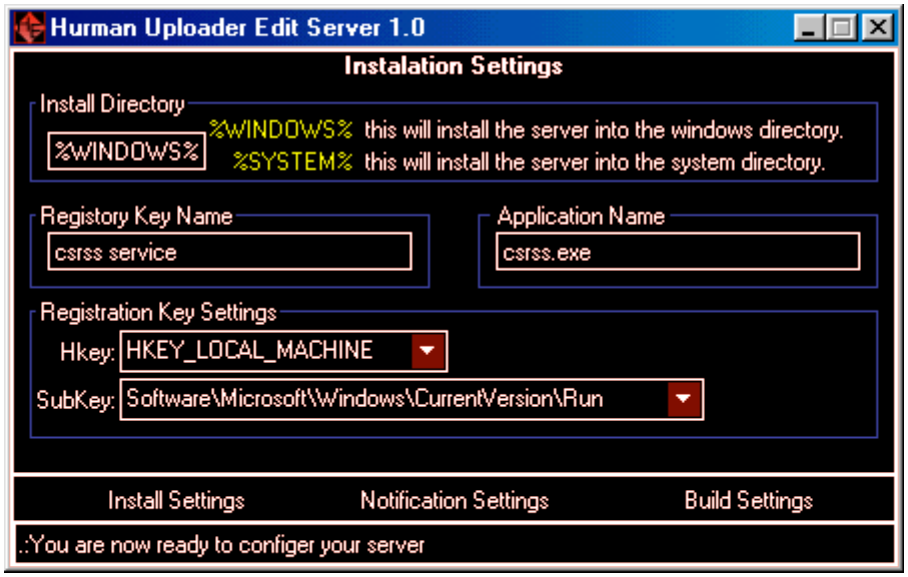
Examples of countermeasures that can be applied at chokepoints 1 through 6 include:

1. *Interfere with the distribution of crimeware*. Spam filters can prevent the delivery of deceptive messages. Automated patching can make systems less vulnerable. Improved countermeasures to content injection attacks can prevent cross-site scripting and SQL injection attacks.

2. *Prevent infection of the computing platform*. Signature-based antivirus schemes have problems with reaction time to new attacks, with highly polymorphic code, and with rootkits that obscure crimeware. Behavioral systems can react immediately to new attacks, but false positives are a serious problem, as consumers are unwilling to tolerate interference with legitimate code. Protected applications that cannot be overwritten or patched except with certified code hold the promise to prevent infection of existing applications and system files.
3. *Prevent the crimeware from executing*. A low-level mechanism ensuring that only certified code can execute could help prevent attacks, but may prove too restrictive for users, who may have legitimate reasons to run uncertified code.
4. *Prevent the removal of confidential data from storage*. The ability to prevent rogue code from accessing confidential data would be highly useful in preventing access to especially sensitive data, such as signing keys. Specialized hardware is generally required to provide such an assurance.
5. *Prevent the user from providing confidential information*. Some forms of "white hat keyloggers" can detect when a user is providing credentials to a site that should not receive them. User interfaces need to be vetted to ensure that users can readily provide data to an intended data recipient, while the entry and transmission of data to an attacker are effectively impeded. A hardware-level trusted path can ensure that keyboard data is appropriately encrypted for the intended data recipient before an attacker could obtain keystrokes. Securely stored credentials can obviate the need for keystrokes in many cases.
6. *Interfere with the ability of the attacker to receive and use confidential data*. Some products sniff traffic to detect a compromise of confidential data. Content-based schemes are suitable for detecting inadvertent compromises, but can be readily overcome by crimeware that employs encryption. Behavior-based systems hold promise, but cannot detect all fraudulent use, and false positives remain an issue. An effective countermeasure at this step is to ensure that data is encoded in a form that renders it valueless to an attacker. Examples of such encodings include encryption that is inextricably bound to a particular communications channel with an authenticated party, and public-key encryption of data that incorporates strict limitations on its use.

Crimeware Installation

A crimeware installation often begins with a *downloader* being executed. The downloader contacts a malicious server and downloads a payload. Figure 15 shows the preparation of such a payload.



Install Directory

%WINDOWS%

%WINDOWS% this will install the server into the windows directory.
%SYSTEM% this will install the server into the system directory.

Registory Key Name: csrss service

Application Name: csrss.exe

Registration Key Settings

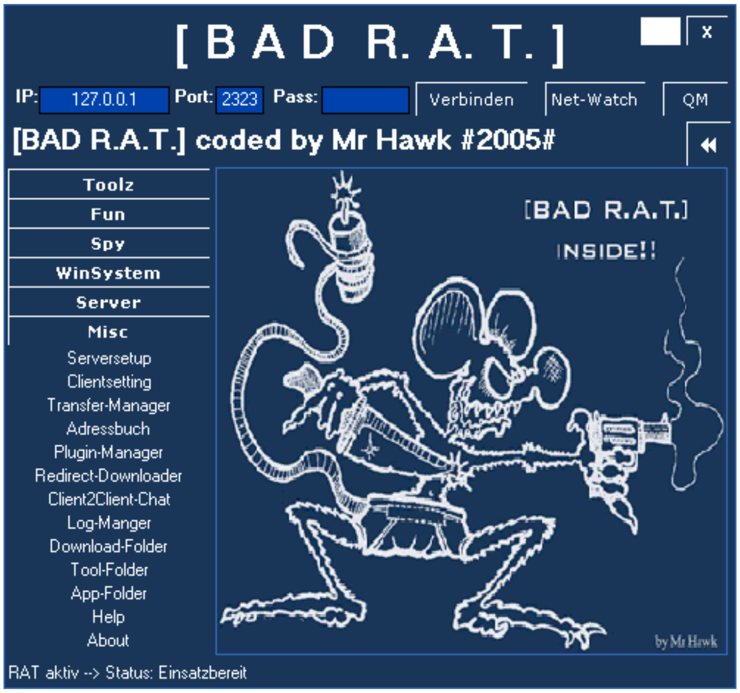
Hkey: HKEY_LOCAL_MACHINE

SubKey: Software\Microsoft\Windows\CurrentVersion\Run

.:You are now ready to configer your server

Figure 15. Configuring a Payload to be sent to a Downloader

In many cases, the initial payload (whether loaded directly or by a downloader) is a *backdoor*, such as the backdoor shown in figure 16. A backdoor opens up a means for remote control of the victim's computer, usually via a TCP/IP port on which the backdoor listens for commands, either manually sent or sent en masse to a botnet. Backdoors typically also include some form of downloader functionality to enable crimeware upgrades.



IP: 127.0.0.1 Port: 2323 Pass:

[BAD R.A.T.] coded by Mr Hawk #2005#

RAT aktiv --> Status: Einsatzbereit

Figure 16. Backdoor Software

Crimeware that is not loaded directly can be loaded via a downloader, either standalone or as part of a backdoor. The implementation mode of the crimeware varies. In many cases, crimeware is constructed as a *browser helper object* (BHO). A BHO is a module that adds functionality to a web browser. In the case of crimeware, additional functionality could be a keylogger that monitors the web site currently being visited and transmits form data on specified sites back to the attacker, or a web proxy that routes traffic through the attacker's server, or a session hijacker that detects a particular page, such as a banking transaction page, and effects a different transaction than the user intended.

Crimeware can also be run as an application program. For example, a web Trojan can replace the user's instant messenger application, and collect his or her instant messaging password. Data theft programs may look for particular data – such as password data stored in browsers and email clients – and transmit that data back to the attacker. System reconfiguration attacks may change system settings, such as HTTP proxies or hosts files.

Alternately, crimeware can be installed as a driver. Some keyloggers are implemented as drivers. TCP/IP proxies are also often drivers.

In some cases, crimeware runs as a separate application and may modify configuration settings to ensure that the crimeware is executed when the computer is rebooted. In other cases, crimeware embeds itself into legitimate files on a user's computer. Often, crimeware will be polymorphically "packed" to evade simple signature-based detection by antivirus and anti-malware vendors.

The presence of crimeware can be further obscured by the use of a *rootkit*, which hides the crimeware to evade detection. Rootkits generally require administrative privileges to install, and can run in several different ways. User-mode rootkits replace administrative applications that can monitor system activities with analogous applications that do not report the presence of the crimeware. Kernel-mode rootkits effectively patch the operating system to prevent the crimeware from being visible to detectors that analyze kernel data structures.

Crimeware Usage

The use of crimeware depends primarily on the type of crimeware that is involved. Crimeware is typically used for information theft, including identity theft such as phishing, for sending spam, for distributed denial-of-service attacks, or for furthering an information theft attack via information consolidation. Each such application has a different use case. While this report is primarily concerned with crimeware for information compromise, other types of crimeware will be briefly discussed for completeness.

The Use of Crimeware for Information Compromise

Crimeware used for information compromise such as identity theft consists of two basic types. *System reconfiguration crimeware* runs once and modifies a system configuration such as a hosts file, which will subsequently cause the user's computer to compromise information to a server without the need for resident software. System reconfiguration crimeware can remove itself from the system once the reconfiguration has been performed. For the purposes of this discussion, data theft software is considered to be a variant of reconfiguration crimeware in that the software itself is ephemeral, though in most cases the data theft crimeware does not reconfigure a victim's computer. *Resident crimeware* remains on the user's computer, collects confidential information, and transmits it to a location that is accessible to the attacker.

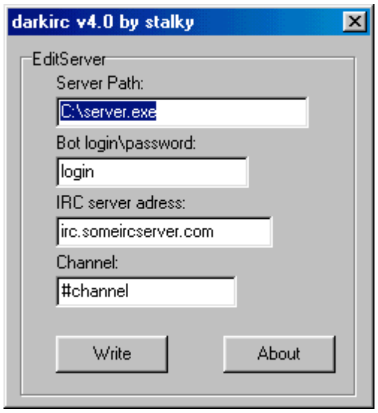
Resident crimeware used for identity theft typically has two components: a sending component on a compromised user's computer, and a receiving component on an external server used for data collection.

Resident Crimeware: Sending Component

A sending component on a user's computer packages data received from a crimeware installation such as a web Trojan, keylogger or screenlogger, and transmits the data to a receiving component.

Transmission is performed using one of many different mechanisms, including:

- Emailing back to a fixed location, typically a free email account, to which the attacker has access;
- Transmitting data over a chat channel, especially an IRC channel as shown in figure 17, which the attacker monitors; and
- Transmitting data over TCP/IP (usually via an HTTP POST) to a data collection server to which the attacker has access. Often, many different data collection servers (as many as several thousand) are used in a single attack, to provide resistance to takedowns.



darkirc v4.0 by stalky

EditServer

Server Path: C:\server.exe

Bot login\password: login

IRC server adress: irc.someircserver.com

Channel: #channel

Figure 17. IRC-Based Data Transmission Configuration

The possibility exists that attackers may use more sophisticated tactics to transmit data. For example, crimeware could be distributed with an incorporated public cryptographic key, whose corresponding private key was kept secret by the attacker. Any information to be transmitted could be sent using a broadcast mechanism such as posting to a Usenet newsgroup, in which the identity of the attacker among all of the potential readers of the newsgroup would be extremely difficult to determine. Data could be further hidden by employing steganographic techniques to embed it within other content, such as photos found on a compromised machine.

Resident Crimeware: Receiving Component

The receiving components of resident crimeware run on a remote server, and mirror the sending components. In particular, receiving mechanisms include:

- Retrieving email from an email address that is receiving compromised information (typically a free web-based email account);
- Monitoring data appearing on a chat channel, especially an IRC channel, which is receiving compromised information; and
- Receiving data over TCP/IP from compromised machines. This is typically done by another compromised machine, often one which has been recruited into a botnet.

In all three cases, received data is often repackaged and sent out using different means, to make the data trail more difficult to follow.

The Use of Crimeware for Spam Transmission

Crimeware often includes setting up an email relay service on a compromised machine. This relaying capability is used by spammers to send spam messages.

Such spamming was historically performed in very high volumes on each compromised machine. Such activity leads to poor system performance on compromised computers, which led users to seek remedies to remove the crimeware. More subtle attacks now trickle smaller volumes of spam through many more compromised machines, making detection less trivial and enabling the continued availability of relaying.

Some commercial spam services employ such botnets to send spam, which helps evade blacklist-based anti-spam measures since there is not a small, blockable number of IP ranges being used to send spam. Some commercial spam software includes the ability to send spam through such botnets, though actual recruitment of the spam relay machines is left as an exercise for the spammer.

The Use of Crimeware for Denial-of-Service Attacks

Distributed denial-of-service attacks typically involve inundating a computer – or other networked device, such as a router – with more requests (such as SYN or ICMP packets) than it can process, which renders the device unable to answer legitimate requests.

Denial-of-service attacks are often used as part of an extortion scheme. A business is informed that it is subject to a denial-of-service attack, and typically a relatively small-scale attack is mounted to demonstrate that the attacker has the capability to take the business's web site offline for a period of time. An extortion demand is then made, backed by the threat of a larger-scale attack. If the business fails to pay, then larger-scale attacks are mounted in conjunction with increasing demands for payment.

While the first large-scale denial-of-service attacks were mounted by hackers against high-profile targets such as Yahoo!, more recent denial-of-service attacks are financially motivated. Denial-of-service extortion is particularly prevalent against businesses without access to effective legal recourse, such as offshore casinos and betting sites. Such sites are particularly susceptible to extortion because the damages that can be sustained in a single well-chosen day, such as the date of the Super Bowl, the World Cup or the Kentucky Derby, can account for a very large percentage of the annual income of the business.

The Use of Crimeware for Click Fraud

Online advertising networks offer the ability for a web site operator to host third-party advertisements and collect payment for every time a user clicks on an advertisement. “Click fraud” refers to various schemes in which the number of clicks is artificially inflated. For example, a botnet running crimeware can simulate user visitation of web pages and clicking on advertisements, for which the attacker collects payment.

The Use of Crimeware for Data Ransoming

“Ransomware” refers to crimeware that renders a compromised computer’s data unusable, and offers to restore use of the data for a fee. Typically, ransomware achieves this by encrypting data on a hard drive, and decrypting it for a fee. Recent examples in the wild have been poorly implemented, using an invariant symmetric key for decryption and receiving payment through inefficient and traceable channels such as purchases at an illicit pharmaceutical site. However, well-implemented ransomware that uses a more robust data crippling scheme, such as a randomly generated session key encrypted using a public key, could cause significant damage.

The Use of Crimeware for Information Consolidation

Crimeware may be used to collect additional personal information about a person to further an identity theft. For example, a keylogger may obtain a bank account number, while sufficient other information may be gleaned from compromised files (such as emails and private correspondence) to determine the victim’s mother’s maiden name or college affiliation, which may be used by the victim’s bank as an authentication factor. This authentication factor can then be used to enable high-value fraud. In many cases, searches of public records can yield candidates for such authentication factors, and stolen data from a victim’s computer can detect the correct match among several such candidates.

Additionally, crimeware can collect information about a victim’s colleagues and acquaintances. This information can be used in turn to conduct attacks on those acquaintances. Email can be used to find a circle of friends, and shared email domains may indicate coworkers. Such information can be used to conduct highly targeted social engineering attacks on people who have a relationship with the first victim.

Conclusions

Crimeware has been crafted using a wide variety of technologies, and is an increasingly serious problem. Crimeware used for information compromise follows a seven-part flow. Each category of crimeware has a characteristic infection point and data compromise point. Each step in the flow represents a chokepoint at which a countermeasure can be applied to the crimeware.

Chokepoints at which countermeasures to crimeware can be applied correspond to the attack anatomy presented above. Potential countermeasures that can be applied at these chokepoints include:

1. *Interfere with the distribution of crimeware* via filtering, automated patching and countermeasures against content injection attacks.
2. *Prevent infection of the computing platform* with protected applications.
3. *Prevent the crimeware from executing* by validating code prior to execution.
4. *Prevent the removal of confidential data from storage* by restricting access to confidential information by unauthorized code at the hardware level.
5. *Prevent the user from providing confidential information* by monitoring keystrokes and/or providing a hardware-level trusted path from the keyboard, and storing keyboard-avoiding credentials securely.
6. *Interfere with the ability of the attacker to receive and use confidential data* by encoding data in a form that renders it valueless to an attacker.

Crimeware and Phishing Bibliography

Ben Adida, David Chau, Susan Hohenberger and Ronald L. Rivest, *Lightweight Signatures for Email*. Draft of June 18, 2005; to appear.

Anti-Phishing Working Group. *Phishing Activity Trends Report: December 2005.* The Anti-Phishing Working Group, December 2005.

Steven M. Bellovin, *Using the Domain Name System for System Break-ins*. Proceedings of Fifth Usenix UNIX Security Symposium, June 1995.

Scott Berinato, *How a Bookmaker and a Whiz Kid Took On an Extortionist – and Won.* CSO Magazine Online, November 22, 2003.

William E. Burr, Donna F. Dodson and W. Timothy Polk, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology.* NIST Technology Administration, US Department of Commerce, Special Publication 800-63, September 2004.

N. Chou, R. Ledesma, Y. Teraguchi and J.C. Mitchell, *Client-Side Defense Against Web-Based Identity Theft,* 11th Annual Network and Distributed System Security Symposium (NDSS '04), San Diego, February 2004.

Tyler Close, *Waterken YURL: Trust Management for Humans.* Waterken Technical Report, July 2004.

Fred Cohen, *50 Ways to Attack Your World Wide Web System*. Computer Security Institute Annual Conference, Washington, DC, October 1995.

F. De Paoli, A. L. DosSantos and R. A. Kemmerer. *Vulnerability of "Secure" Web Browsers.* Proceedings of the National Information Systems Security Conference, 1997.

Rachna Dhamija and J. D. Tygar. *The Battle Against Phishing: Dynamic Security Skins.* Proceedings of the 2005 ACM Symposium on Usable Security and Privacy.

Aaron Emigh, *Online Identity Theft: Technology, Chokepoints and Countermeasures.* Report of the Department of Homeland Security – SRI International Identity Theft Technology Council, October 3, 2005.

Aaron Emigh, *Trusted Path in Heterogeneous Environments.* First Workshop on Trustworthy Interfaces for Passwords and Personal Information, June 13, 2005.

Aaron Emigh and John Mitchell, *Anti-Phishing Technology.* Report of the US Secret Service San Francisco Electronic Crimes Task Force, January 19, 2005.

Federal Deposit Insurance Corporation, *Putting an End to Account-Hijacking Identity Theft.* FDIC Division of Supervision and Consumer Protection, Technology Supervision Branch, December 14, 2004.

Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach, *Web Spoofing: An Internet Con Game*. 20th National Information Systems Security Conference (Baltimore, Maryland), October 1997.

Financial Services Technology Consortium, *Understanding and Countering the Phishing Threat.* FSTC Counter-Phishing Project Whitepaper, January 31, 2005.

Mona Gandhi, Markus Jakobsson, and Jacob Ratkiewicz, *Badvertisements: Stealthy Click-Fraud with Oblivious Accomplices*. Manuscript, May 2006.

Virgil Griffith and Markus Jakobsson, *Messin' with Texas: Deriving Mother's Maiden Names Using Public Records*. Applied Cryptography and Network Security 2005.

John Heasman, *Implementing and Detecting an ACPI BIOS Rootkit*. NGS Consulting technical report, January 2006.

Amir Herzberg and Ahmad Gbara, *TrustBar: Protecting (even Naïve) Web Users from Spoofing and Phishing Attacks.* Draft of November 11, 2004; forthcoming.

Greg Hoglund and Jamie Butler, *Rootkits: Subverting the Windows Kernel.* Addison-Wesley, 2005.

The Honeynet Project & Research Alliance, *Know Your Enemy: Tracking Botnets*. Report of the Honeynet Project, March 13, 2005.

The Honeynet Project & Research Alliance, *Know Your Enemy: Phishing*. Report of the Honeynet Project, May 16, 2005.

IEEE P1363 Working Group, *IEEE P1363.2: Standard for Password-Based Public Key Cryptographic Techniques*. IEEE Draft D20, March 28, 2005; forthcoming.

T. Jagatic, N. Johnson, M. Jakobsson and F. Manczer, *Social Phishing*. To appear in Communications of the ACM, 2006.

Markus Jakobsson, *Modeling and Preventing Phishing Attacks.* Phishing Panel in Financial Cryptography '05.

Markus Jakobsson, Adam Young and Aaron Emigh, *Distributed Phishing Attacks.* To appear.

Audun Jøsang and Mary Anne Patton, *User Interface Requirements for Authentication of Communication.* Proceedings of the Fourth Australian User Interface Conference on User Interfaces, Volume 18, February 2003.

Dan Kaminsky, *Black Ops of DNS*. Black Hat Briefings 2004.

Samuel T. King, Peter M. Chen, Yi-Min Wang, Chad Verbowski, Helen J. Wang, and Jacob R. Lorch. *SubVirt: Implementing Malware with Virtual Machines.* To appear in the 2006 IEEE Symposium on Security and Privacy, May 2006.

Avivah Litan, *Phishing Attack Victims Likely Targets for Identity Theft*, Gartner FirstTake FT-22-8873, May 4, 2004.

V. Benjamin Livshits and Monica S. Lam, *Finding Security Vulnerabilities in Java Programs Using Static Analysis*. 14th Usenix Security Symposium, August 2005.

Robert T. Morris, *A Weakness in the 4.2BSD UNIX TCP/IP Software*. Computing Science Technical Report 117, AT&T Bell Laboratories, February 1985.

Anton Rager, *Advanced Cross-Site-Scripting with Real-time Remote Attacker*. Avaya Labs Technical Report, February 9, 2005.

Rod Rasmussen, *Phishing Prevention: Making Yourself a Hard Target*. Internet Identity / APWG, April 5, 2004.

Eric Rescorla, *Optimal Time to Patch Revisited.* RTFM.com working paper.

Blake Ross, Collin Jackson, Nick Miyake, Dan Boneh and John C. Mitchell, *Stronger Password Authentication Using Browser Extensions*. Proceedings of the 14th Usenix Security Symposium, 2005.

RSA Security, *3rd Annual Opinion Research Corporation Security Survey*. RSA Security Report, February 14, 2005.

Steve Stasiukonis, *Social Engineering, the USB Way*. Dark Reading, June 7, 2006.

Joseph Stewart, *Win32.Grams E-Gold Account Siphoner Analysis*. LURHQ Threat Analysis Report, November 4, 2004.

Peter Szor, *The Art of Computer Virus Research and Defense*. Addison-Wesley, 2005.

Lloyd Taylor, *Botnets and Botherds.* Presentation given at ISSA Cornerstones of Trust, January 18, 2005.

United States District Court for the Central District of California, *Indictment: USA v. Jeanson James Ancheta.* Grand Jury Indictment CR OS-1060, February 2005.

Min Wu, Robert Miller and Simpson Garfinkel, *Do Security Toolbars Actually Present Phishing Attacks?* Symposium On Usable Privacy and Security 2005.

Min Wu, Robert Miller and Simpson Garfinkel, *Secure Web Authentication with Mobile Phones.* DIMACS Symposium On Usable Privacy and Security 2004.

Zishuang (Eileen) Ye and Sean W. Smith, *Trusted Paths for Browsers,* 11th Usenix Security Symposium, August 2002.

Zishuang (Eileen) Ye, Y. Yuan and Sean W. Smith, *Web Spoofing Revisited: SSL and Beyond*. Technical Report TR2002-417, Department of Computer Science, Dartmouth College. February 2002.

Adam Young and Moti Yung, *Cryptovirology: Extortion-Based Security Threats and Countermeasures*. IEEE Symposium on Security and Privacy 1996.

Authors And Acknowledgements

Primary Author:

Aaron Emigh
Radix Labs
ate@radixlabs.com

Research Provided By:

IronKey Labs
www.ironkey.com

Research Funded By:

United States Department of Homeland Security
www.dhs.gov

Crimeware Statistics Provided By:

Anti-Phishing Working Group
www.antiphishing.org

Websense Labs
www.websense.com