# Anatomy of an Intrusion

Insider's look at a real, sustained attack against a major, multinational corporation

Shari Lawrence Pfleeger, RAND Corporation IT Pro July/August 2010

Dr. Panayotis Kikiras INFS 150 University of Thessaly Oct 2015

- The company under attack has several thousand employees located around the world
- Its central server is located in the US
  - and supports thousands of end-user systems,
  - 200 to 300 other servers,
  - and two main Internet access points.
  - also supports customers and the general public

Much of the company's work involves

databases of information that it must protect and separate from other parts of the network

- One portion of the network has substantial security requirements, including government classification of data.
- Other data sets aren't classified but are sensitive
- and must be carefully protected

The IT staff originally designed the network

to support users' and customers' needs for functionality, with little regard for security except when explicitly required.

- All corporate staff have laptop or desktop computers with local administrator privileges.
- Many of the corporate employees and customers require remote access to the network

- Because of the diversity of work location access ranges from highspeed linkage to dial-up.
- All remote offices send traffic to the central site.
- Ninety percent of the resources are at the central site, and only some remote offices provide IT support.
- Typically, traffic volume is high in the morning, drops mid-morning, and is up again at noon, often reflecting when the staff at remote sites gets to work and logs on to read email. There are major drops in volume over the weekend, but the volume is never zero.

# **Discovering the Attack**

- The IT support staff was the first to notice something wrong.
- One domain controller, started acting strangely restart itself for no apparent reason.
- Called Microsoft for help
- Luckily, they have a red –team exercise from an outside vendor
  - During the exercise, the participants discovered that real attackers were present on port 8080 an adversary was shipping rogue system files to an external destination.

# The million dollar Question

Can you imagine where?

Hacked By Chinese Hacker - Microsoft Internet Explorer	コンロン学をす	
Edit Yess Fguarites Iaak belp		
🖂 · 🔘 · 🖻 🗟 🚳 🔎 Search 👷 Ferrurken 🕘 🚔	• 🚳 🖂 • 💭 એ 🕸 🕮 🥙	
iene 🕢 Marthemandarakb.com.cn/		× 🔂 😡 📢
Chines	se Ho	acker
林純学変勢を力売時時に無外絶回め、台湾見十四下ゴクが約 」また時に1997年にくられらようまたパリケット のまたにからのは下からのまたよいにしたまた。 のまたがいていたいたとりに見ついます。	407. IIBLERSLERARTEORUS. HR ADJELIANIJOZIRIVAZIENIJOZUJELEBE GODBITUR-ADJELISIII ZOZUNIJU INIJUZI	客状記~の主式原料の名葉論:「 な作の元一 合す器!!!! REVTOTSULTPEF3)XSSEEDORTISTEP BSD-KiLTOLAIBYTAVILBSCTALSE こちULSEYYAVILBSCCTALSE こちULSEYYAVILBSCCTALSE
TSALUYUU SUUGUT I ALYMLIXAI YDW YDW YGDOSIOGAADGCYDEGSBGAEYCIGYPOLDEI GSDUNUWYXJELINGCIDU GOESTALIAA	PEDEAL PROCESSING AND LINES PROJECTION OF THE FIL	CCBY9905TTCQVISOQQL3133E542138 PAD 0990D3CL58F91VLID1362,38630 JUTIJUD762830005E697265371847
CT26ACRIDCCR7_OPTVEA2HDADNTRE CG220RPTX2220RCCVCR4EDCE15PQ	4005790915610073879005894204917	2.JC 10P: STORNMASY 20ATT EXCEPTIO DONING CONTINUES TO DO
T7X3301R617301T400720YXCR5T04 T775675895464G30005009ML4831 Y87306M64090012714570420137	USYNS 2015 THIM WESTRED COST AND A DECEMPTING THE PROPERTY SET TO THE STREET AND A DECEMPTING AND A DECEMPTI	ELECTOR SALEY PORSENCE OF CHEMISSING EAJE 600 60 YHE SCHWY IGY 7000 398 57 YED IND DIVITION AS CONVOLUTION
0TL#C10F22500135TL3465A2L10 1101 ESLOB403991238M/22330827EM45 ESECT100F11434970M/223308238	SAMAGAGI SHISHIDITKI PJANKI POKLANSKI PI 11.1 SAMANY20 SOTTTINDI 2598647 MAJANUAN 2171.	LOWERALSEDASSWIDTSLANDOUTS IFFOMSSP4594L08920SVTLDCOMFG ITFOMSSP4594L08920SVTLDCOMFG
YOREAL RESVELLED FURATESALD 400 STYTTESKISSISJAJEP EXCELSED 50	CCSECLOREF300F5-3533770F2.3-11,000 CCSEEW16F7E90372:0E02265122DT0-44_EY0	13/DEEL25/2190550C2R134151E-0 FEL72/VR(PTUKSMEEALL51MEGTAY
04783053279363016353470007103 0478254203411357774641655127491 362304620963678870027530651048670	PV DDPAN E- DDP 1	AF490HECK(9,20031ASYT26E)6D0K
KS DOC 160 RTO 3915 2000 RAA 91 LEN ACC BE 70 46 209 GOC 3918 ROTE GOOD GOOD GOOD GOOD ACC KS DOC 160 RTO 3915 2000 RTA 91 LEN ACC	The         HEDRONIC         1123-112           The         HEDRONIC         1123-112           The         HEDRONIC         1123-112           The         HEDRONIC         1123-112	d infolt 3 systems first systems c2.7m Ray Rowert Synaps 2006 for Paral Systems Sincolt 3 systems first systems c2.7H
2019-536 LL 8778 RAJ 17 AR 00286 870 77 SYND SIVSEY DOCUMENTS OF BRIDE 1	WESTERN ASSOCIATE DI 2023/19/0 (1981-00/00/10/10/00/00/27) (* 0/00/00/27)	ACINERCHIPSYYLLAS2714678397237971 ACINERCHIPSYYLLAS2714678397237971
BERGING BUNKER DE TOUR PRESENDE BURE PERMOUND DE DE DE DE SOCIETAS SOCIETAS BURE PERMONENTE SOCIETAS SOCIETAS DE	0749Y9 001 0125 0125 0125 0125 0125 0125 0125	CION CTSTRENDUIST 40C250C6871 6E271774L INTTSTPERMERATY VENNSS INT 2017422046
HPROGUN034.0001.1731040471203040 077140255771.056057 7134705019983.9760404720405.37711	ENVDYGHIBSNGLKLTELL 6649G31CB5AADSV9FTL 6649G31CB5AADSV9FTL	Iduar Volva ShF5538CH I HERENIGTH CSSCREEL F750CMBTAQ4827F1 CSSCFCHT
«LVER242/UBPC_DTR2200206F20/FF40 CTSFTML3887/HL2EUR837MEX2F6SV50BT TTTF1UL66238C07LTTC58762F65V50BTC8	PEDALDHEAKS TOPOMITIKAN 74 TOURTWOODSPROT FILESCH 231 ON DOURTWOODSPROT FILESCH	KZZENISTOPNIKATBZATBZANISYZSEBTEYO DYVDEZIITIXSOIZSISHAWASIIRZSIN CSACSWISTISHCAMELATEPCKIZHONKUP
IFLEMMORYCFED-MILEYS, SPALEYY, SPACE 653C5A6VI304LKC3D06FKAIAFH/IIID76 72F9SCT3S0FF0475A504VA0C21749I31474	TYPTA IN INTER 25 THE INCOMMENDED STORATED EFERST ARTSTDOAPSCLIDE STWARTING 12200-1 INTERACTOR INTERCOMPLETED STRATTING	82224100-CTVTEWONCOCLOSESSENTYTW 80-FCN0-0CTANTED-INFITTD-5-4C3W3EA 81.1198-03-CNE-0M-040011-2719-9357A
44F13D000G3c1V22GP0F7T1B5L0VG0CT 34F13VE260UECC_3560FT6R1/2042EA0F31 B0706C0M521SM03DE1BV2007E059F0700	NALDA LASTRINI, 2010 INDER SOLUTION SSLEDT THE ISLAMANE SOLUTION AND AND AND AND AND AND AND AND AND AN	LET YES ONE DOUBLO PYCE BOLD CYCS ID LET NEWS Y YENERS JUL 35 SUT PY (NBUB NY TYUL FENN NAC JUL 25 SUT PY (NBUB
BGP0Q+0D-S7CY12F(1+0CY5LERIS// 1 SZFU2LES-1002Y, TY3PP1EPS, TADA ANDR DSTVD27, TY3PP1EPS, TADA ANDR	CV10011D20CE11V10VF3214910V5ARE*A52240 967Q02191M2REF911F72R9611CED7003287F33 0000310TK12003000148C667TM1V0806897439	STARACED VT 2 SOOD OD CHCYNCT 47111 FO NE BYPE 1052 I YSDURBUT 1951A SUPEG TRECT STUTTP FAMA FOR ONLY 1951A SUPEG
IREPTINA CORDITION LEIGEFTC Tideltar Toutei Japier (C.D.) X304174735400 T.P.COMERCOIT A	IRENZ HIM TO 400 IREVEZYOSKAPE IRTOWERE IROQ TO FAJER KOROKEZI - DYNGOWYZSAC O APANOXO PO IOG D/41 POXOTEDONE IU4 OYEMI 2KVMSOT / 7N IOXO	EXEMPLE CONTRACTOR SECTIONS OF A CONTRACT OF
12459200000000 1359943374828895 27594000440405587885976889768807112977	KER JOODS PROKI BERGTOKO JUDGUBN SNI OLANA AAA KER JOODS PROKI BERGTOKO JUDGUBN SNI OLANA AAA	PETEIBSOLESELUE 210012711900 IOHISZSSIANFISLSSSSS214U29UI

Percen the decide of the

# **Discovering the Attack**

- These assaults were quite sophisticated

   not the typical automated virus or denial of service.
- the attacks were targeted
  - were looking for specific information from people with expertise in particular areas
  - malicious software planted on corporate computers involved key loggers

# First Reaction

- the company took steps to reduce unauthorized data leaving its systems
- the attackers responded with a massive effort to scan corporate networks for vulnerabilities.
- mandate that all employees reset their passwords to something that had not been used before
- increased the volume of help-desk calls to over
- 3,000

# Handling the Attack

- Disconnect the system from the Internet
- observe background traffic for anomalous behavior (create own email, DNS directly out)
- Scan databases (sun solaris)
  - an open source rootkit tool found

## X-Raying the Attack

- What mechanisms enabled the attack?
  - Targeted, customized Trojans were used in the attackers' first strike.
- The Trojans arrived in several different ways,
- including
  - when staff opened a malicious email attachment, typically a Word file, PDF file, or spreadsheet;
  - when staff intentionally or inadvertently went to a malicious website;
  - when staff or a process opened a malicious file transmitted on a hard medium (such as a CD or thumb drive) or using a network protocol (such as FTP)
  - when a process accessed a company computer.

## X-Raying the Attack

- Malware typically arrived in an email and,
   once enabled, sent and received data using a
   Domain Name System (DNS), HTTP, and HTTPS.
- Malware's most telling symptom was the change in network traffic
- The company uses three separate layers of antivirus protection from three separate vendors, none identified the Trojans.

# Attack Enablers

- **Microsoft Word** was an important vector for the Trojans.
  - Even though all company computers had updated personal firewalls, antivirus software, spyware, and operating system patches, they didn't have updated Microsoft Office patches.
  - because the attacks were persistent and changing, sometimes the adversary exploited a vulnerability for which no patch was yet available.

# Attack Enablers

- A combination corporate of factors enabled attacks' success:
  - Using the network for collaboration
  - Using email to share information
  - Employees moving frequently from one site to another
- many workers felt that the technology
- would protect them
- —so they focused more on getting their jobs done than on protecting their equipment and data.

# Mitigating the Effects

- Mandating a proxy for Web browsing
- Requiring two-factor authentication
- Reducing update times
- Hardening operating systems and applications
- Investigating malware in attachments
- The company also hired staff with some forensic experience

# Mitigating the Effects

- The short-term goal was twofold:
  - increase the work factor (that is, make the attackers work harder to compromise a machine) and
  - focus on behavior instead of signature- or rule-based discovery.
- Network-behavior monitoring tools support the search for unusual behavior

#### Addressing the Long-Term Threats

- When the company took the steps just described, the unauthorized flow of data from the corporate network was significantly reduced and eventually eliminated
- the attackers fought back with a massive scan of vulnerabilities in the public-facing corporate systems.

#### Addressing the Long-Term Threats

- Create new business and security Policies
- Resulting to a timeline and cost estimation
- Furthermore they decided to comply with the following strategy

# Ten Steps Toward Security

- Run Red-Team Exercises
- Update the Security Plan
- Review Processes (Both business and Security)
- Develop Customized Tools
- Use Outside Experts.
- Increase Network Segmentation (create a "cold room" for extra – sensitive data)
- Continue System Hardening

# Ten Steps Toward Security

- Enhance Security Awareness
- Remove Local Administrator Privileges
- Address Insider Threats (honeypots)



"Now there is more of a tilt toward security. The attack opened our eyes. Before the attack, we had never meditated deeply on where the balance between service and security should be."