Tempest: Ein Signal Problem

Übersetzung aus freigegeben Materialien der NSA

Die Geschichte der Entdeckung
der verschiedenen Strahlungen zu beeinträchtigen
von Kommunikations-und Comsec Ausrüstung.

Im Jahr 1962, ein Offizier zu einem sehr Smajl Intelligenz zugeordnet
Ablösung in Japan war er die Übung Pflicht
Untersuchen Sie den Bereich um seine kleine cryptocenter. Als
erforderlich, wurde er der Prüfung einer Zone mit einem Radius von 200 m zu sehen,
ob es eine "geheime technische Überwachung."
Auf der anderen Straßenseite. vielleicht hundert Meter entfernt, war ein
Krankenhaus von der japanischen Regierung kontrolliert. Er
schlenderte an einer Art von Carport hinausragende von einer Seite
Das Gebäude und, bis unter dem Dach, bemerkte einen eigentümlichen
Ding-a sorgfältig verborgen Dipol-Antenne, horizontal
polarisiert. mit führenden Leitungen durch den Feststoff cinderblock
Wand, die das Carport anliegt. Er moseyed zurück zu seinem
Hauptsitz, dann schnell die Spionageabwehr benachrichtigt
Menschen-und ausschalten, einen Bericht von diesem gefeuert "finden", um Armee-
Sicherheitsbüro
Agentur, die. wiederum benachrichtigt NSA. Er wurde gerichtet
untersuchen diese Antenne im Detail und vielleicht erholen, aber
obwohl die Spionageabwehr Leute hatten versucht,
halten den Carport unter Beobachtung in dieser Nacht, die Antenne
hatte auf mysteriöse Weise verschwunden, wenn sie das nächste überprüft
Tag. Oben auf dem Dach des Krankenhauses war ein Wald von der Vagi,
TV-Antennen, die alle auf in Richtung Tokio in der normalen
Mode, mit einer Ausnahme. Dass man wurde gleich zu U, S. gerichtet
cryptocenter.

Vielleicht erinnern Sie sich die stark beachteten Klappe, die
im Jahr 1964 aufgetreten, wenn mehr als 40 Mikrofone waren
entdeckt in der US-Botschaft in Moskau. Die meisten Leute
wurden über all die Gespräche, die möglicherweise betroffenen
belauscht worden, und die resultierende Kompromiss unserer
diplomatische Pläne und nachrichtendienstliche Tätigkeiten im Zusammenhang mit
Die Botschaft. Wir wurden um etwas anderes:
Was könnten diese Mikrofone zu tun, um die cryptomachines
verwendet es? Und was waren die unpublirized Gadgets auch

gefunden mit Mikrofonen für? Warum gab es eine große Metall-
Gitter vorsichtig in den Zement von der Decke über der vergrabenen
Department of State Kommunikationsbereich? Ein Gitter mit einer
Draht führt irgendwohin. Und was war der Zweck der
der Draht, der in einem sehr feinen Netz aus kleineren Haar beendet.
wie Drähte? Und. wenn wir schon dabei waren, wie hat diese Funde
beziehen sich auf andere geheimnisvolle Funde und Berichte von hinten
die Curtain-Berichte aus dem Jahr 1953 klar?

Warum, Weg zurück in 1954, als die Sowjets eine veröffentlichte
recht umfassende Reihe von Standards für die Unterdrückung
von HF-Störungen, waren diese Standards viel
strengere für ihre Fernschreibmaschinen und
Kommunikationsgeräte als für solche Dinge wie
Diathermie Maschinen, industrielle Motoren und dergleichen, auch
obwohl die Fernschreiber waren viel ruhiger in der ersten
Ort?

Hinter diesen Ereignissen und Fragen liegt eine lange Geschichte
beginnend mit der Entdeckung einer möglichen Bedrohung. die langsame
Erkennen einer Vielzahl von Variationen dieser Bedrohung
und, schwerfällige entlang ein paar Monaten oder wenigen Jahren
danach, um eine Reihe von Gegenmaßnahmen zu reduzieren oder zu eliminieren
jede neue Schwäche, die offenbart worden ist.

Das Problem definiert

Um den allgemeinen Charakter der Probleme in Kürze angeben:
Jedes Mal, wenn eine Maschine verwendet, um zu verarbeiten klassifiziert wird
Informationen elektrisch, die verschiedenen Schalter, Kontakte.
Relais und andere Komponenten in dieser Maschine kann emittieren
Hochfrequenz oder akustische Energie. Diese Emissionen, wie
winzige Radiosendungen. Mai strahlen durch den freien Raum für
beträchtliche Strecken-eine halbe Meile oder mehr in einigen Fällen.

Oder sie können auf dem nahe gelegenen Dirigenten wie Signal induziert werden
, Stromleitungen, Telefonleitungen, oder Wasserleitungen und sein
durchgeführt, entlang dieser Pfade in einiger Entfernung, und hier
können wir von einer Meile oder mehr reden.

Wenn diese Emissionen können abgefangen und aufgezeichnet werden,
ist es oft möglich (0 analysieren sie und erholen das
Intelligenz, die durch die Quelle verarbeitet wurde
Ausrüstung. Das Phänomen betrifft nicht nur die Chiffre
· Maschinen, sondern jede Information-Processing
Geräte-Fernschreiber. Duplizieren von Ausrüstung,
inrercornms, Fax, Computer-you name it. Aber es ist
besondere Bedeutung für cryptomachines weil es wolle
legen nicht nur die Ebene der einzelnen Texte menages sein
verarbeitet, sondern auch, dass sorgfältig gehüteten Informationen über
die internen Abläufen an der Maschine. Somit ist vorstellbar, die
Maschine werden könnte strahlende Informationen die dazu führen könnten
zum Wiederaufbau unserer täglich wechselnden Keying
Variablen-s-und aus einer Comsec Sicht ist das absolut
das Schlimmste, was uns passieren kann. Dieses Problem der
kompromittierende Abstrahlung haben wir die covername gegeben

Tempest.

Entdeckung von Bell Lab

Nun, gehen wir zurück zum Anfang. Im Ersten
War II, das Rückgrat für Armee und Marine sichere
Fernschreiber Kommunikation waren einmalig und Bänder
die primitive Krypto-Geräte SIGTOT. Zum Verschlüsseln
die Dienstleistungen verwendet einen Bell-Telefon Mischvorrichtung, genannt
Ein 13 I-B2. Wenn eine dieser Mischer wurde in getestet
eine Bell Labor. ein Forscher bemerkt, ganz zufällig,
dass jedes Mal die Maschine trat, erschien ein Spike auf ein
Oszilloskop in einem entfernten Teil des Labor. Nachdem er untersucht
diese Spitzen mehr sorgfältig. er fand, er könne die Lese-
Klartext Ofthe Nachricht, die durch The Maschine verschlüsselt!

Bell Telephone in einem Dilemma. Sie hatten die verkauft
Ausrüstung für das Militär mit der Gewissheit, dass es
zu sichern, aber es war nicht. Das einzige, was sie tun konnte, war
sagen rhe Signal Corps darüber. was sie auch taten. Dort
trafen sich die Gründungsmitglieder einer dub der Skeptiker, könnte
nicht glauben, dass diese winzigen Kerne wirklich ausgenutzt werden könnte
unter praktischen Feldbedingungen. Angeblich sind sie zu haben
sagte etwas wie: "Weißt du nicht, es ist Krieg?
Wir können nicht bringen unsere kryptographischen Operationen ein
Vollbremsung auf der Grundlage einer zweifelhaften und esoterischen Labor
Phänomen. Wenn dies wirklich gefährlich, es beweisen. "Also. Die
Bell-Ingenieure wurden in einem Gebäude auf Varick Street in plaziert
New York. Auf der anderen Straßenseite und etwa 80 Meter entfernt war
Signal Corps 'Varick Street cryptocenter. Die Ingenieure
aufgezeichneten Signale für etwa eine Stunde. Drei oder vier Stunden
später produzierte sie etwa 75% der Klartext, das war

Sein verarbeitet-eine schnelle Performance, nebenbei bemerkt, hat das
nur selten erreicht worden. .

. Das Signal Corps wurde von diesem Display beeindruckt und
directed Bell Labs, um dieses Phänomen eingehend zu untersuchen
und bieten Modifikationen an der 131-B2-Mischer zu unterdrücken
die Gefahr. In einer Angelegenheit von sechs: Monate oder so, hatte Bell Labs
identifiziert drei verschiedene Phänomene und schlug drei
grundlegende Unterdrückung Maßnahmen:

(A) Abschirmung (für Strahlung durch den Raum, und
magneticfields)
(B) Filtern (für leitungsgebundene Signale auf Stromleitungen,
Signalleitungen, etc.)
(C) Maskieren (entweder für Raum abgestrahlt oder durchgeführt
Signale, vor allem aber für die Raumfahrt)

Bell Labs ging voran und verändert einen Mixer, nannte es
Die I31-A-1. In ihr sie benutzt sowohl die Abschirmung und Filterung
Techniken. Signal Corps warf einen Blick auf sie und wandte sich
Daumen runter. Das Problem war. um die Straffälligkeit enthalten
Signale, hatte Bell zu kapseln praktisch die Maschine.
Anstelle einer Nachrüstung, die sich auf das Gebiet besent könnte,
Die Maschinen müssten zurückgeschickt werden und rehabilitiert.
Die Kapselung verursacht Probleme der Wärmeableitung.
Wartung extrem schwierig gemacht, und behindert
Operationen, indem der Zugriff auf die verschiedenen Kontrollen.

Statt für den Kauf dieses Monster, griff die Signal Corps
auf die einzige andere Lösung, die sie denken konnte. Sie gingen
heraus und warnte Kommandeure des Problems, riet ihnen
, um eine Zone etwa 100 Meter im Durchmesser zu kontrollieren um ihre
Kommunikationszentrum, um verdeckte Abhören zu verhindern. und
lassen es dabei bewenden. Und die Cryptologic Gemeinschaft als Ganzes
lassen es dabei bewenden für die nächsten sieben Jahre oder so. Der Krieg
endete, die meisten der beteiligten Personen ging zurück zu zivilen
Leben, die Dateien im Ruhestand waren, zerstreut und zerstört. Die
ganze Problem wurde anscheinend vergessen. Dann, in 195 L,
Das Problem war, für alle praktischen Zwecke, durch wiederentdeckt
CIA, als sie mit der gleichen alten 131-B2 liebäugelt
Mischer. Sie berichteten, gelesen zu haben Klartext über ein
Viertel Meile auf der Signalleitung und fragte, ob wir waren
interessierten. Natürlich waren wir. Einige Versorgungs-und Signalleitungen
Netzfilter gebaut wurden und sofort auf diese installiert
Ausrüstungen und sie hat den Job ganz gut so weit wie
durchgeführt Signale waren betroffen. Kosmische Strahlung
ungebrochen jedoch fortgesetzt und die erste von vielen
"Strahlung" Politik wurde in Form eines Briefes von ausgestellt
AFSA allen SIGINT-Tätigkeit, von ihnen zu verlangen:

1. Steuerung eine Zone 200 Fuß in alle Richtungen um
die cryptocenters oder
2. Betreiben Sie mindestens 10 TTY-Geräten gleichzeitig
(Die Idee der Maskierung; Außerbetriebnahme einer solchen Fülle von
Signale, dass eine Überwachung und Analyse schwierig sein würde), oder
3. Holen Sie sich einen Verzicht auf die operative Notwendigkeit basiert.

Die Sigint Gemeinde so gut es ging angepasst, und
in einigen Fällen. Allgemeine Service-Kommunikatoren angenommen
ähnliche Regelungen. Die Zahl von 200 Fuß. übrigens war ziemlich
willkürlich. Es war nicht bestimmt worden, weil wir hart hatte
Beweise dafür, dass. in größerer Entfernung. Interception war
unpraktisch, sondern. es war der größ ~ t
Sicherheitszone wir
glaubte die Mehrzahl der Stationen vernünftigerweise mainrain,
und wir wussten, dass, mit Instrumentierung dann in Anspruch nehmen.

in der Lage, die Ausbeutung zu diesem Bereich würde im besten Fall sein überaus schwierig.
Zur gleichen Zeit, dass wir versuchten, mit der Bewältigung
13)-B2-Mischer. fingen wir an, jede andere Chiffre untersuchen
Maschine. Everytbing 'tested abgestrahlt. und strahlte eher
überaus produktiv. Mit Rotor-Maschinen. die Spannung an ihren
Stromleitungen eher als eine Funktion der Anzahl schwankt
der Rotoren bewegen. und sogar eine vierte Phänomen, das als
Ausgießer Linie modllaltion, entdeckt wurde.
j Die Fortschritte bei der Prüfung der Maschinen und die Entwicklung
ij Unterdrückung Maßnahmen war sehr langsam. Bis 1955 jedoch eine
Anzahl der möglichen Techniken zur Unterdrückung der
Phänomene versucht worden. FiJterin8 Techniken waren
etwas verfeinert; Fernschreiber Geräte wurden so modifiziert
dass AU Relais gleichzeitig betrieben und nur eine einzige Spitze war
produziert mit jedem Charakter, anstelle von fünf kleineren

Spikes. Darstellen jedes Baud, aber die Größe des Dorns
verändert mit jedem Charakter produziert, und die Analysten

\ Konnte noch las es schnell. Eine "ausgewogene" Zehn-Leiter-System
II wurde versucht, das würde jede ausgestrahlte Signal zu erscheinen
identisch sind. aber zur Erreichung und Erhaltung solcher Ausgewogenheit bewiesen
unpraktisch. Hydraulik-Techniken, um das zu ersetzen
Ich elektrische-waren ausprobiert und verworfen, und Experimente
! wurden mit verschiedenen Arten von Batterien und der Motor aus
~ Enerators.
in Versuchen, die Power-Line Problem zu lecken.
Keiner war sehr erfolgreich.
Während dieser Zeit das Geschäft der Entdeckung neuer
TEMPEST Bedrohungen. oder an technischen Verbesserungen und
Instrumentierung für derecting, Aufzeichnung. und Analysieren
diese Signale, schneller fortgeschritten als die Kunst des
unterdrücken. Vielleicht ist der Angriff ist spannender als
die Verteidigung etwas mehr Glamour-über das Finden eines
Weg eines dieser Signale als der Weg über die Lese
Plackerei notwendig, um zu unterdrücken, dass whacking großer Dorn
erste im Jahr 1943 gesehen. Auf jeden Fall. wenn sie sich über die

nächsten Felsen. sie fanden das akustische Problem unter ihm.
Phenomenon Nr. '5.
~ I
Akustik
Wir fanden, dass die meisten akustischen Emanationen Lire schwer zu
machen, wenn die microphonic Gerät außerhalb des Raumes
mit der Quelle Ausrüstung, auch ein Stück Papier
eingefügt zwischen, sagen wir, einer Straffälligkeit keyboa.rd und einer Pick-up
Gerät ist in der Regel genug, um zu verhindern, ausreichend genaue
Aufnahmen auf Ausbeutung zu ermöglichen. Schrotflinte
Mikrofone-the Art verwendet werden, um abholen ein Quarterback der
Signale in die Köpfe zusammen und großen Parabolantennen sind

effektiv bei der Hunderte von Füßen-wenn es einen direkten Schuss auf die Ausrüstung. Die akustische Bedrohung ist also. beschränkt für diese Anlagen, wo die verdeckten Abfangjäger bekommen können irgendeine Art von Mikrofon-wie ein normales Telefon Das wurde in abgehört oder links aus dem Schneider-in der gleichen Raum mit der Informationsverarbeitungsvorrichtung. Wir haben auch entdeckt, dass, wenn der Raum "schalldicht" ist mit gewöhnlichen akustischen Welle, die Aufgabe der Ausbeutung ist einfacher weil die Schall-Schnitte nach unten reflektiert und hallenden Klang, zur Klärung der Signale. Ein beunruhigender Entdeckung war, dass gewöhnliche Mikrofone. wahrscheinlich gepflanzt abholen Gespräche in einem cryptocenter. erkennen konnte, Maschine klingt mit genügend Treue zu ermöglichen Ausbeutung. Und wie Mikrofone wurden in entdeckt Prag. Budapest, Warschau und natürlich. Moskau.