Ingegneria della conoscenza

‘Ottobre Rosso’ un esempio di Cyber-spionaggio

ANTONIO TETI

Red October, nell’immaginario collettivo di molti, identifica un famoso film degli anni ‘90 in cui Sean Connery interpretava il comandante di un sottomarino russo in fuga dall’Unione Sovietica. Oggi identifica qualcosa di diverso da una preda in fuga negli abissi marini: un temibile ‘cacciatore digitale’ del Cyberspazio…

Operazione ‘Red October’: ed è Cyber Espionage

Ottobre 2012. I ricercatori del Kaspersky Lab Global Research & Analysis Team, avviano un’intensa attività di ricerca e analisi su alcune minacce provenienti dalla rete, in funzione della rilevazione di alcuni attacchi informatici indirizzati su reti di computer di diverse strutture diplomatiche. Nel giro di qualche settimana, i tecnici di Kaspersky si imbattono in una *botnet*[1] che si distingue dalle altre per le spiccate finalità spionistiche che persegue. È rapidamente battezzata ‘Red October’, che riporta alla mente il celebre film del 1990, ‘Caccia a Ottobre Rosso’, diretto da John McTiernan e tratto dall’omonimo romanzo di Tom Clancy. Contrariamente alla trama del film, che attribuiva a un futuristico e silenzioso sottomarino sovietico il ruolo di ‘preda’, in quanto inseguito da altri sottomarini dello stesso paese intenzionati a distruggerlo, nel caso del *maliciuos code* Red October, è lui ad assumere il ruolo di ‘cacciatore’ conservando, però, la stessa silenziosità e aggressività del sommergibile del film. E, a quanto è dato sapere, pare che abbia esercitato questo ruolo per 5 lunghi anni, prima di essere scoperto da una serie di accurate indagini iniziate a partire dal 2007. Va rilevato che a gennaio 2013, risultava essere ancora attivo.

[1] Botnet. È una rete formata da computer collegati ad Internet e infettati da software maliziosi in grado di danneggiare un sistema informatico. Una botnet si può creare grazie alla presenza di falle di sicurezza nei computer o nella rete, oppure per negligenza da parte degli utenti o dell’amministratore del sistema. In questo caso, i computer vengono attaccati e infettati da virus informatici che consentono, ai loro creatori, di controllare l’intera rete da sistemi remoti. I controllori della botnet possono sfruttare i computer infetti per scagliare attacchi distribuiti del tipo *distributed denial of service* (DDoS) contro altri sistemi in Rete e possono condurre ulteriori azioni criminose, alle volte agendo persino su commissione di organizzazioni criminali. I computer che compongono la botnet sono chiamati bot (da roBOT) o zombie.

Il nome attribuitogli, così come sottolineato dall'azienda russa Kasperksy, è però riconducibile al luogo in cui ha avuto origine il network che ha scatenato le azioni di cybercrime: la Russia. Ma va evidenziato che molti dei server che si sono resi protagonisti degli attacchi, sono dislocati in altri paesi europei, come, ad esempio, la Germania.

Nella relazione tecnica presentata da Kaspersky, risulta che gli attacchi si sono estesi a macchia d'olio dall'Asia fino agli Stati Uniti, attaccando principalmente strutture istituzionali, governative (le ambasciate in particolare), accademiche e, soprattutto, centri di ricerca ubicati prevalentemente in Europa orientale e in Asia centrale. La *mission* principale dei cyber-criminali, era finalizzata alla raccolta di informazioni inerenti le tipologie di sistemi informativi oggetto degli attacchi, i dispositivi mobili ad essi collegati (notebook, netbook, smartphone, iPad), le differenti varietà di apparecchiature di trasmissione indirizzamento di dati in rete (switch, firewall, router), e non ultimo per importanza, alcuni database memorizzati nelle memorie di massa dei sistemi informatici.

La tecnica utilizzata è la seguente: inizialmente, i *crackers*[2] raccolgono una serie di informazioni utili sul bersaglio da colpire, utilizzando una tecnica di *phishing*[3] particolarmente raffinata: lo *spear phishing*. È un programma appositamente sviluppato per scagliare attacchi di phishing, ma solo dopo aver preliminarmente raccolto informazioni dettagliate sul bersaglio.

Un esempio classico di *spear phishing* è quello che vede il destinatario dell'attacco ricevere una mail da un mittente 'noto' o 'conosciuto' (quindi valutato come innocuo), in cui sono allegati documenti apparentemente reali e riconducibili al lavoro che il ricevente svolge o che sono riferibili alla sua vita personale. Di conseguenza, la mail assume tutte le caratteristiche di un messaggio vero e affidabile. In seguito è introdotto un codice malizioso (malware[4]) opportunamente creato per condurre determinate azioni (trafugare dati e informazioni, bloccare i sistemi, modificare i dati memorizzati nei computer, cancellare dati e programmi, ecc). In questo caso, il codice malizioso è strutturato per acquisire i dati contenuti nei diversi computer presenti nella rete in cui si è introdotto, fino a colpire perfino i dispositivi di telefonia mobile (smartphone) ad essi collegati. Secondo quanto affermato dai tecnici di

[2] Cracker. In ambito informatico il termine cracker identifica un esperto informatico che utilizza le sue conoscenze e tecnologie per aggirare le barriere e i sistemi di protezione (hardware e software), per conseguire vantaggi, il più delle volte, economici. Tuttavia il cracking può essere finalizzato anche allo spionaggio militare, industriale o per le truffe o per alimentare la disinformazione. Il termine cracker viene spesso confuso con quello di hacker, il cui significato è tuttavia notevolmente diverso. L'hacker è colui che sfrutta le proprie conoscenze per esplorare, valutare o testare un sistema informatico, senza tuttavia creare danni o inefficienze al sistema.

[3] Phishing. È una tecnica di truffa in rete mediante la quale un attaccante pensa di ingannare la vittima convincendola a fornire informazioni personali sensibili. Uno dei classici esempi è quello dell'invio causale di messaggi di posta elettronica che imitano la grafica web di siti bancari o postali. Con questa tecnica, il cyber-criminale cerca di ottenere dai malcapitati le username e le password di accesso al sistema.

[4] Malware. In informatica, il malware sta ad indicare un qualsiasi software realizzato con lo scopo di danneggiare un computer o una rete di sistemi informatici. Il termine deriva dalla contrazione delle parole inglesi *malicious* e *software* e ha, dunque, il significato letterale di 'programma malvagio' o 'codice maligno'.

Kaspersky, sarebbero circa 3.000 i dispositivi caduti nella trappola di Red October e dalle loro memorie sarebbero stati trafugati documenti altamente riservati. Uno degli aspetti maggiormente inquietanti, risiede nella tipologia dei files dati che sarebbero stati prelevati dai sistemi attaccati: i files rubati includerebbero quelli con estensioni *txt, csv, eml, doc, vsd, sxw, odt, docx, rtf, pdf, mdb, xls, wab, rst, xps, iau, cif, key, crt, cer, hse, pgp, gpg, xia, xiu, xis, xio, xig, acidcsa, acidsca, aciddsk, acidpvr, acidppr, acidssa*. Va rilevato che le estensioni 'acid', sono riconducibili a uno specifico software applicativo dal nome 'Acid Crypto - filer' che è utilizzato da molteplici enti ed organizzazioni istituzionali, tra cui l'Unione Europea e la NATO e il francese Département Maîtrise de l'Information (ex Centre Electronique de l'Armement, CELAR). Pertanto, è plausibile ritenere che i sistemi di Red October siano in grado di decifrare sia i messaggi che i documenti cifrati da Acid Cryptofiler.

Secondo l'indagine condotta dall'azienda russa, sono quattro i punti salienti su cui si sarebbe basata l'intera operazione:

1. Gli attacchi si sono protratti per almeno cinque anni, e sono stati rivolti prevalentemente contro agenzie diplomatiche e governative di mezzo mondo. Molte delle informazioni raccolte sono state utilizzate per condurre nuovi attacchi, come nel caso del trafugamento delle credenziali di accesso ai sistemi di utenti di particolare importanza, che inserite in specifici elenchi, sono state utilizzate per individuare le password di accesso ad altri sistemi ubicati in reti diverse. Un particolare interessante risiede nel sistema di 'pilotaggio' dei computer infetti: per esercitare il loro controllo si è dovuto procedere alla creazione di oltre sessanta *nomi di dominio*[5] e altrettanti server (computer di rete) dislocati in diversi paesi, di cui una buona parte ubicata in Germania e Russia. Inoltre, si è reso necessario creare un'infrastruttura C&C (Command & Control) basata sul funzionamento di una 'batteria' di server che aveva funzionalità di *proxy*[6] e di reti *VPN*[7] (figura 1) per nascon-

[5] Nomi di dominio. Il sistema dei nomi a dominio (Domain Name System, DNS), è un sistema utilizzato in Internet per la risoluzione di nomi dei *nodi* della rete (host) in indirizzi IP (Internet Protocol number) e viceversa. Il servizio è realizzato tramite un database distribuito in rete, costituito dai server Domain Name Server.

[6] Server proxy. Un server proxy è un programma che si interpone tra client (utente) e un server (computer di rete), e può essere utilizzato sia in locale sia per l'accesso diretto ad Internet. In quest'ultimo caso, è possibile avere alcuni client, con indirizzo IP pubblico, che si connettono ad un server con funzione di proxy, il quale gestisce le richieste per conto loro: il risultato, è una connessione anonima per ogni client connesso tramite il proxy.

[7] VPN (Virtual Private Network). Una VPN è una tecnologia che permette il collegamento fra due reti private attraverso la rete pubblica, ed è nata fondamentalmente con l'obiettivo di instaurare una connessione criptata, e di aumentare così la produttività delle aziende. Attraverso una VPN è possibile creare una connessione fra il pc di un utente ed un server remoto VPN, e tutti i dati in transito, attraverso Internet, sono inviati all'interno di un tunnel virtuale (tunneling), criptato ed inaccessibile da chiunque. Il server remoto VPN poi si occupa di agire come server proxy, nascondendo quindi l'identità dell'utente. Molto spesso, questa tecnologia è utilizzata per trasportare i dati di un utente in un luogo geograficamente diverso da quello di partenza, assoggettato il più delle volte a leggi diverse.

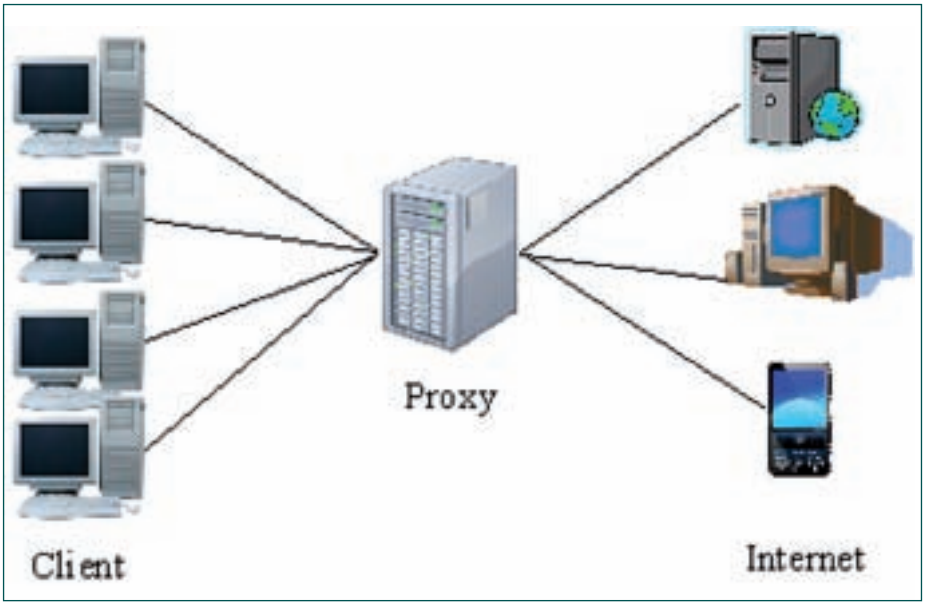

Figura 1. *Comunicazione tramite Proxy*

dere gli indirizzi IP dei server di comando e controllo (mothership) da cui partono le direttive per le azioni di attacco.

2. I crackers di Ottobre Rosso hanno creato una struttura poliedrica e multifunzionale in grado di condurre attacchi basati su tecniche particolarmente efficaci e performanti ma, soprattutto, finalizzate a condurre attività di cyber-intelligence. Inoltre il sistema C&C si è rivelato particolarmente resistente alle azioni di intercettazione, oltre a rivelarsi straordinariamente efficace nel ripristinare il collegamento ai server infetti (che venivano protetti dai sistemi di difesa delle vittime) attraverso canali di comunicazione alternativi.
3. Oltre ai canonici sistemi informatici (computer, server e workstation diverse), gli attacchi hanno interessato anche i dispositivi mobili, come gli smartphone (in particolare iPhone, Nokia e i terminali che utilizzano Windows Mobile), ma anche i dispositivi attivi di rete (in particolare quelli dell'azienda Cisco). Inoltre sono state condotte azioni di prelevamento di files (dati) da memorie di massa removibili, ivi comprese le informazioni cancellate (ma recuperabili grazie all'utilizzo di software speciali), ancora memorizzate all'interno dei supporti violati. Sono stati, altresì, rubati i database di posta elettronica di molti *mail server* (computer che gestisce la posta elettronica), oltre ai dati contenuti in numerosi file-server (computer adibiti alla memorizzazione di archivi di dati).
4. Gli attacchi sono stati indirizzati anche verso alcuni programmi applicativi di Office Automation della Microsoft. È stato rilevato l'utilizzo di tre

diversi *exploit*[8] impiegati per violare i seguenti applicativi di uso comune: CVE-2009-3129 (MS Excel), CVE-2010-3333 (MS Word) e CVE-2012-0158 (MS Word). Alcuni erano già noti sin dal 2010 (MS Excel) altri sono apparsi nel 2012 (MS Word). In pratica, il codice maligno è stato trasmesso per e-mail, come allegati di files di Word, Excel ed anche in formato PDF.

Per quanto concerne l'azione del prelevamento di informazioni, nel momento della ricezione del *malware*, attivato dall'apertura del documento da parte della vittima e sfruttando le vulnerabilità di sicurezza riscontrate, si attiva una procedura di 'search and picks' che trasmette istantaneamente le informazioni ricercate al sistema C&C.

Secondo i dati aggiornati da Kaspersky a gennaio 2013, i computer infetti superavano i 300 (figura 2).

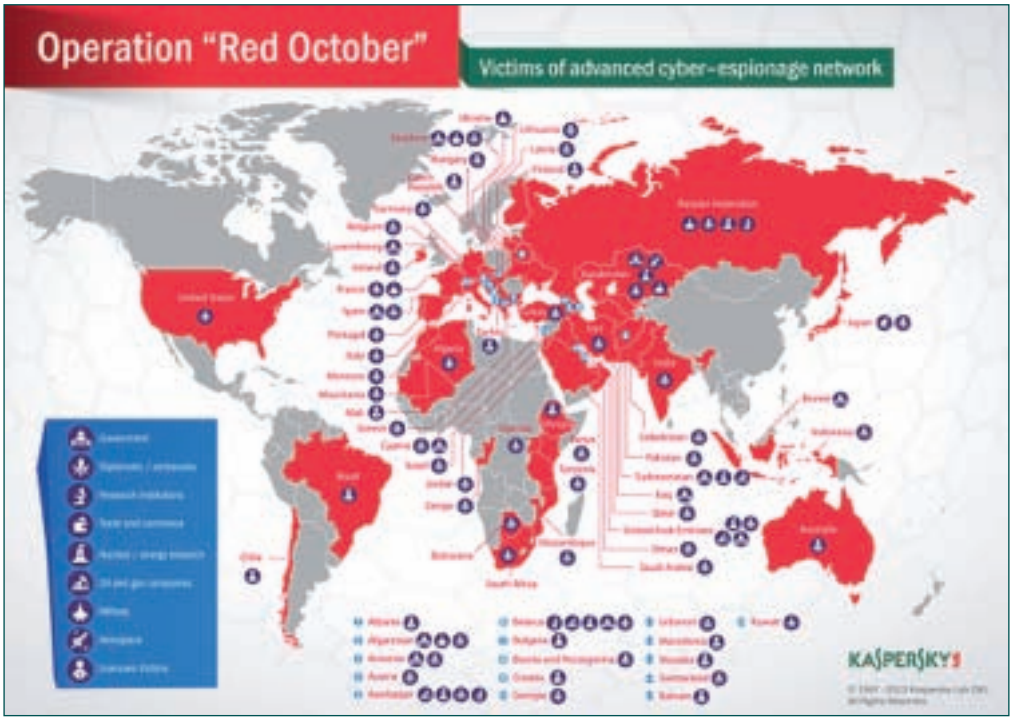

Figura 2. *Le vittime di Ottobre Rosso*
(fonte www.securelist.com/en/images/pictures/klblog/208194085.png)

[8] Exploit. Nel gergo informatico, serve ad identificare un codice (programma) che, sfruttando una vulnerabilità di un sistema, consente di acquisire dei privilegi (accesso completo al sistema) o a produrre dei malfunzionamenti al sistema stesso.

Ma l'aspetto più critico rilevato dai tecnici dell'azienda russa, risiede nella straordinaria capacità del *malicious code* di Ottobre Rosso di penetrare i computer e di prelevare tutte le credenziali di accesso (username e passwords) memorizzate al suo interno. Inoltre, è stato accertato che riesce a rilevare tutti i device driver collegati tramite interfacce di collegamento diverse (USB, wireless, IrDA e Bluetooth) ai computer violati, grazie all'utilizzo di *keylogger*[9].

Essendo ormai diffusa la pratica di collegare smartphone e pen-drive USB ai computer, si evince istantaneamente quale possa essere, in termini numerici, l'estensione dell'intera operazione di trafugamento di dati.

Una volta acquisiti, i dati sono inseriti in pacchetti 'sporchi' (pacchetti dati che contengono informazioni generiche e insignificanti) e trasmessi a circa 60 server di C&C, molti dei quali ubicati in Germania. Questi ultimi, come atto finale, comunicano con i server di vertice, definiti anche con il termine di 'navi madre' (mother ships), mediante l'utilizzo di proxy che si fanno carico della trasmissione dei dati, in modalità completamente anonima. '*Il tutto è strutturato come una buccia di cipolla*' asserisce Rave Costin Raiu, trentenne a capo di un particolare team di ricerca di Kaspersky, che può contare sulla disponibilità ed efficienza di 34 'supertecnici' informatici, geograficamente dislocati in località diverse del pianeta, ma che dirige dal suo ufficio di Bucarest.

Nel tentativo di scoprire il punto di origine di Red October, Raiu crea un programma specifico per identificare le vittime del codice maligno. È una tecnica che si basa sull'assunzione degli indirizzi dei web server che non hanno 'risposto' ai tentativi di accesso degli aggressori. In sostanza Raiu tenta di assumere l'identità (IP number) di una delle possibili vittime ancora da attaccare, deviando il traffico dati nel suo laboratorio. È una tecnica conosciuta con il termine di *sinkhole*[10], e che consente all'utente di osservare, in profondità, i *tunneling* in Rete. Dopo poche settimane erano state catalogate 55.000 richieste provenienti da computer contaminati. '*Siamo stati solo in grado di accedere a sei dei sessanta server di Comando*' ha asserito Raiu, '*In altre parole, siamo riusciti a vedere solo circa il 10 per cento della rete*'. Ciò è dovuto in gran parte alle interruzioni delle azioni di Ottobre Rosso operate dai server C&C per mettere il software maligno 'in letargo', con lo scopo preciso di disinnescare le azioni di intercettazione. Ciò tuttavia non deve lasciar intendere che gli attacchi siano definitivamente cessati, dato che Ottobre Rosso può essere riattivato in qualsiasi momento.

[9] Keylogger. In gergo informatico, il keylogger è un dispositivo di *sniffing* (attività di intercettazione passiva dei dati), hardware o software capace di intercettare tutto ciò che un utente digita sulla tastiera del proprio, o di un altro computer.

[10] Sinkhole. Un DNS Sinkhole, noto anche come un Sinkhole Server, è un server DNS (Domain Name Server) che fornisce informazioni false per impedire l'uso dei nomi di dominio veri. L'utilizzo più comune è quello di bloccare le Botnet (una rete formata da computer collegati ad Internet e infettati da malware, controllati da un'unica entità, il botmaster), interrompendo i DNS utilizzati da una Botnet. È una tecnica che può essere utilizzata sia per difendersi da attacchi che per condurli.

Un altro aspetto interessante risiede nel fatto che, dopo l'accesso al sistema, il codice maligno attiva ben 1000 applicazioni software con il solo scopo di condurre azioni di Cyber-Intelligence. Raiu ha eseguito un test all'interno del suo laboratorio proprio per verificare l'efficacia di queste azioni: dopo aver infettato un computer, il virus ha mappato l'intera rete del laboratorio e ha stilato un elenco dettagliato di tutti i dispositivi informatici presenti, ivi compresi i dispositivi attivi di rete (*switch, router, firewall, proxy*). Successivamente, ha archiviato tutti i dati raccolti, cifrandoli in appositi file. Poi ha proceduto all'assegnazione di un numero per ogni sua vittima (computer). Terminato il lavoro di analisi, catalogazione e memorizzazione delle informazioni, il computer infetto ha proseguito mettendosi in contatto una serie di server dislocati sulla rete Internet.

È proprio in questo momento che inizia la trasmissione dei dati a indirizzi di rete 'fasulli', grazie all'utilizzo del proxy. Sarà quest'ultimo, a reindirizzare i pacchetti dati alle 'navi madre'.

Altro aspetto interessante è dato dalla poliedricità e multifunzionalità dei malware: in funzione della tipologia di piattaforma hardware/software da attaccare, il computer infetto utilizza i software più adeguati, conducendo attacchi simultanei su sistemi diversi. Quindi, i software procedono con la ricerca di password, documenti particolari, informazioni contenute nei database, elenchi di dati, tabelle, ecc. Se sono identificati elenchi con numeri telefonici, alcuni software procedono con i tentativi di accesso ai terminali mobili (smartphone) tentando di collegarsi in modalità Wireless, WiFi, Bluetooth o con chiamate telefoniche dirette. Si presuppone che, queste applicazioni maliziose siano anche in grado di copiare i dati contenuti nei telefoni cellulari, ivi comprese le informazioni cancellate.

A questo punto potrebbe sorgere la seguente domanda: com'è possibile che nei cinque anni di attività di Ottobre Rosso, le innumerevoli applicazioni antivirus fruibili sul mercato non siano state in grado di rilevare l'esistenza di questo worm[11]? Una possibile risposta la fornisce Andreas Marx, amministratore delegato di AV-Test[12], noto istituto tedesco specializzato in sicurezza informatica, che asserisce: '*Ottobre Rosso infetta solo singoli computer in maniera molto mirata, mentre il software anti-virus, di solito, si concentra su worm diffusi*'.

Ottobre rosso ha indirizzato gli attacchi principalmente verso la Russia ed altre repubbliche ex sovietiche, ma sono stati infettati anche molti computer in India, Afghanistan e in particolare in Belgio, dove hanno sede l'Unione Europea e la NATO. Meno infezioni sono state riscontrate negli Stati Uniti, l'Iran, Svizzera e Italia.

[11] Worm. Un worm (traducibile dall'inglese come 'verme') è una particolare categoria di codice maligno la cui sua maggiore peculiarità, risiede nella capacità di autoreplicarsi. È molto simile ad un virus, ma si differenzia da quest'ultimo per il fatto che non ha bisogno di altre applicazioni per diffondersi.

[12] www.av-test.org/en/home/ .

Non sono state riscontrate infezioni in Cina e in Corea del Nord.

Inoltre è singolare che, secondo quanto affermato dal team dell'azienda russa, Red October presenti vistose somiglianze con i famigerati codici maligni *Stuxnet*, *Flame* e *Gauss*, che hanno, di fatto, inaugurato negli anni scorsi l'era delle Cyberwar.

Cyber Intelligence: la nuova frontiera dello spionaggio

Vitaly Kamlyuk è un bielorusso di 28 anni, componente della 'special unit' di Kaspersky che ha contribuito alla scoperta di Ottobre Rosso. In un'intervista rilasciata al quotidiano tedesco online Der Spiegel[13], asserisce che dagli attacchi condotti è emerso '*… un interesse speciale per informazioni significative a livello geopolitico*'. Sempre secondo il tecnico bielorusso, sembrerebbe che sia stata proprio l'Ambasciata Russa l'obiettivo più ambìto degli attacchi.

E a quanto è dato sapere, sono stati migliaia i documenti (si parla di terabyte di dati), ivi compresi quelli 'classificati' del Ministero degli Esteri a Mosca, a cadere nelle mani delle cyber-spie. Pare che il silenzioso *sottomarino digitale* abbia trascorso i suoi primi cinque anni a setacciare, analizzare, controllare, assimilare e memorizzare informazioni di ogni tipo, ed è quasi certo che la maggioranza delle sue vittime non si siano accorte di nulla. '*Noi non abbiamo mai visto prima di ora un attacco condotto con tale precisione chirurgica*' asserisce Kamlyuk. E c'è da crederci, poiché l'azienda per cui lavora non riesce ad accumulare informazioni aggiuntive sul *malware*, perché '*… il nemico sta distruggendo le prove*', grazie al passaggio allo stato di 'offline' dei sistemi di controllo e pilotaggio degli attacchi.

Come abbiamo potuto comprendere, Ottobre Rosso appartiene alla famiglia dei software maliziosi, denominata da Kaspersky con il nome 'Sputnik', in grado di infettare i computer che utilizzano applicazioni come Word ed Excel, sfruttandone le vulnerabilità nascoste. Forte di circa un migliaio di *malware* (raggruppati in moduli), i ricercatori di Kaspersky, hanno catalogato almeno 10 categorie di azioni dannose (moduli) che possono essere indirizzate sui computer attaccati:

1 *Recon (Reconnaissance)*. Sono moduli progettati per essere utilizzati durante la fase iniziale dell'attacco, dopo la fase di penetrazione dei sistemi informatici. Il loro scopo principale è quello di *raccogliere* informazioni generali sull'obiettivo, per poter localizzare e identificare i computer da infettare, per stimare il valore potenziale dei dati informatici disponibili e per definire quali altri moduli debbano essere utilizzati in seguito.

[13] http://www.spiegel.de/international/spiegel/how-russian-virus-hunters-tracked-down-a-global-espionage-network-a-879467.html .

Queste applicazioni si occupano anche della raccolta di ulteriori informazioni in grado di fornire indicazioni interessanti, come la cronologia del siti web visitati, le credenziali di accesso memorizzate nella *cache* del *browser* (username e password), e le eventuali impostazioni di client FTP[14].

2 *Password*. Sono moduli in grado di estrarre le credenziali (username e password) da una serie di programmi, tra cui la cartella temporanea protetta di *Microsoft Outlook* (posta elettronica, rubrica contatti, appuntamenti, attività) e *Agent Mail.ru*, il più popolare portale di posta elettronica gratuita utilizzato da *Runet*[15]. Inoltre, questi moduli, sono in grado di raccogliere l'*hash*[16] dell'account di Windows per consentire di penetrare qualsiasi workstation.

3 *E-mail*. In questa categoria troviamo i moduli per estrarre i messaggi e i dati memorizzati localmente dai *client* di posta elettronica come *Outlook* e *Thunderbird*, ma anche per le connessioni da remoto (POP3) o su server di posta (IMAP). Riescono a copiare l'indirizzo del mittente, del destinatario/i, il testo del messaggio e perfino i file contenuti all'interno degli stessi (*attach*).

4 *USB Drive*. Sono moduli capaci di sottrarre dati dalle unità che si collegano alle interfacce USB (pen drive, memorie di massa, smartphone, pc, ecc.). Possono raccogliere qualsiasi tipologia di files e possono persino acquisire un intero *file system*[17], inclusi i files cancellati.

5 *Keyboard*. Sono moduli capaci di registrare le battiture su tastiera. Sono programmi che registrano le lettere e i numeri che sono digitati, memorizzando tutto ciò che è immesso nel sistema, ovviamente ivi comprese le credenziali di accesso riservate, catturando perfino le immagini proiettate sullo schermo (in tal senso l'abbinamento tra applicazioni e battiture è automatico).

[14] Client FTP. È un software che consente di utilizzare la funzione di file transfer (File Transfer Protocol, FTP) per trasferire files dati da un computer all'altro.

[15] Runet. È un termine molto utilizzato che identifica i siti web e i domini Internet riconducibili alla Russia. Viene spesso utilizzato dai media come sinonimo di rete russa.

[16] Hash. Nel campo informatico, corrisponde ad una funzione che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita. Le funzioni hash svolgono un ruolo essenziale nella crittografia e per la creazione di firme digitali.

[17] File System. In gergo informatico, identifica un meccanismo con il quale i file sono organizzati e archiviati in una memoria di massa, come un disco rigido o un CD-ROM. Identifica anche l'insieme delle tipologie di dati necessari per la memorizzazione (scrittura), l'organizzazione gerarchica, la manipolazione, la navigazione, l'accesso e la lettura dei dati.

6 *Persistence*. Ne fanno parte i moduli che procedono all'installazione di codici *payload*[18] per applicazioni diverse (*Word*, *Acrobat Reader*, ecc.), oltre a *plugin*[19] utilizzati per riprendere il controllo di computer precedentemente compromessi, che possono essere stati parzialmente disinfettati.

7 *Spreading*. Sono moduli che consentono di eseguire la scansione degli *host* (terminale collegato alla rete, solitamente un computer) di una rete locale, infettandoli mediante l'utilizzo di credenziali già estratte in precedenza o per organizzare attacchi che si basano sulle vulnerabilità riscontrate. Un esempio tipico di attacco è quello indirizzato contro i *router*[20] per acquisire le tabelle d'instradamento dei pacchetti dati trasmessi in rete.

8 *Mobile*. Moduli innovativi e temibilissimi, sono in grado di copiare tutte le informazioni presenti negli smartphone che si interfacciano ad una rete utilizzando una qualsiasi modalità di trasmissione dati. Alcuni moduli possono verificare se un dispositivo è *jailbroken*[21] e utilizzarne la funzione per introdurre *malware*.

9 *Exfiltration*. Sono moduli che intercettano e prelevano tutti i dati memorizzati sulle memorie di massa di server di tipo FTP (computer identificabili come *file server*, utilizzati per veicolare e memorizzare dati diversi condivisi in rete), per ritrasmetterli poi a server di comando (*C&C server*). Solitamente si attivano dopo l'azione dei moduli che rientrano nella categoria *Recon*.

10 *USB Infection*. Anche se non sono stati riscontri effettivi sulle loro capacità, sembra che questi moduli siano stati creati per attaccare direttamente le unità USB[22], mandando in esecuzione dei virus sui dispositivi collegati mediante queste interfacce.

La maggiore delle peculiarità dei malware di Sputnik, risiede nell'altissimo livello di sofisticazione delle applicazioni, un elemento che conferma l'esi-

[18] Payload. È una *runtime* (momento in cui un programma per computer è eseguito) presente in un virus informatico che ne estende le funzioni oltre l'infezione del sistema. Si intende con *payload,* quindi, qualsiasi operazione a tempo determinato, casuale o attivata da un comando contenuto all'interno di un virus o worm. L'azione del payload può essere di distruzione parziale o totale di informazioni, la loro diffusione non autorizzata, l'invio di email a tutti gli utenti della rubrica oppure azioni similari.

[19] Plugin. È un programma autonomo che interagisce con un altro programma per ampliarne le funzioni (ad esempio un plugin su un programma di scrittura che consente di attivare una funzione per la quale è necessario un altro programma).

[20] Router. Traducibile con il termine di instradatore, corrisponde ad un dispositivo elettronico che, all'interno di una rete informatica, si occupa di instradare i dati suddivisi in pacchetti (pacchetti dati) fra reti diverse.

[21] Jailbreaking. È una procedura che permette di installare su un dispositivo tipo smartphone, applicazioni che consentono di acquisire programmi alternativi a quelli presenti sul dispositivo (ad esempio alternativi all'App Store). Dopo aver effettuato il jailbreak sul dispositivo, gli utenti possono installare numerose applicazioni altrimenti non disponibili tramite l'App Store.

[22] USB. Universal Serial Bus.

stenza di un'infrastruttura di tecnici informatici di altissima specializzazione, diretti da *team leaders* (in questo caso esperti di intelligence), in grado di fornire indicazioni precise sulle tipologie di azioni che le applicazioni devono condurre, oltre ad individuare gli obiettivi da colpire.

In sostanza è semplicemente inconcepibile che si possa ritenere che dietro un'operazione così complessa ed articolata, si celi uno sparuto gruppetto di hackers in cerca di emozioni o un raggruppamento isolato di cybercriminali indipendenti, al soldo del miglior offerente. Dietro Ottobre Rosso si cela un'imponente infrastruttura gerarchica di tipo militare, strutturata in sezioni, aree di competenza e personale con specializzazioni diverse, in grado di definire obiettivi specifici, azioni mirate e finalità da conseguire. Un'infrastruttura complessa di queste dimensioni, deve anche poter contare su finanziamenti di non poco conto, indispensabili per l'acquisizione di dispositivi informatici di grandi prestazioni e particolarmente innovativi.

È, altresì, improbabile che una struttura così complessa e imponente, possa sfuggire all'attenzione di strutture governative o istituzionali. Di conseguenza, se ne deduce che, un apparato di Cyber Espionage come quello che ha realizzato Ottobre Rosso, non possa operare senza la diretta collaborazione, se non addirittura integrazione, con strutture governative o organizzazioni che operano in stretto contatto con uno Stato.

Chi si cela dietro Ottobre Rosso?

Ottobre Rosso può essere considerato come il primo autentico programma sviluppato per azioni di tipo *spyware*, cioè in grado di condurre azioni di spionaggio in Rete.

La sua maggiore peculiarità risiede nella sua capacità di trafugare informazioni 'classificate' e non banche dati comuni o di scarso interesse. Da ciò deriva il sospetto che dietro questo temibilissimo strumento d'intelligence digitale, si possa celare il servizio segreto di un paese particolarmente all'avanguardia nel settore della Cyber Intelligence.

Anche se in questo momento il 'committente' e gli 'autori' degli attacchi restano ancora avvolti nel mistero, qualche indizio trapela dall'analisi del codice di Ottobre Rosso. Innanzitutto, tra le righe del programma è possibile leggere parole come '*zakladka*' (termine russo utilizzato per identificare un *bug*), oppure '*proga*' (sempre in russo, identifica la parola *programma*), che lasciano intuire che dietro il gruppo di sviluppatori del codice maligno si celino crackers russi. Sergei Nikitin, esperto di sicurezza informatica del Governo di Mosca, ritiene che il programma sia stato commissionato da '*un servizio di intelligence che ha assunto programmatori attraverso forum nella comunità di hacker russi*'. Ma potrebbe trattarsi anche di un'azione di simulazione per indurre gli analisti a conclusioni completamente errate.

Non è certo una novità quella dell'apertura di un nuovo mercato di professionisti della guerra digitale. I *mercenari digitali* (cyber-mercenaires), rappresentano i nuovi 'soldati' del terrorismo informatico internazionale del terzo millennio. Alle armi e agli esplosivi, preferiscono le tastiere e il mouse che, oltre ad essere inesauribili al contrario delle armi, sono enormemente più economiche e garantiscono danni che possono rivelarsi anche più efficaci e devastanti delle più sofisticate e costose armi disponibili sul mercato.

Ma torniamo per un istante a esaminare l'architettura di Red October. Se la analizziamo attentamente, possiamo giungere alla conclusione che si tratta della prima operazione che prevede l'interazione tra cyber-spie e cyber-criminali a livello transnazionale. Come? Cerchiamo di comprenderlo ripercorrendo alcuni passaggi focali.

Innanzitutto partiamo dalla metodologia di attacco e infezione.

A settembre 2012, grazie ad una vulnerabilità del *browser* di navigazione Internet Explorer di Microsoft ('IE zero-day' exploit), sono attaccati numerosi computer in tutto il mondo, e la campagna di azioni di cybercrime presen-

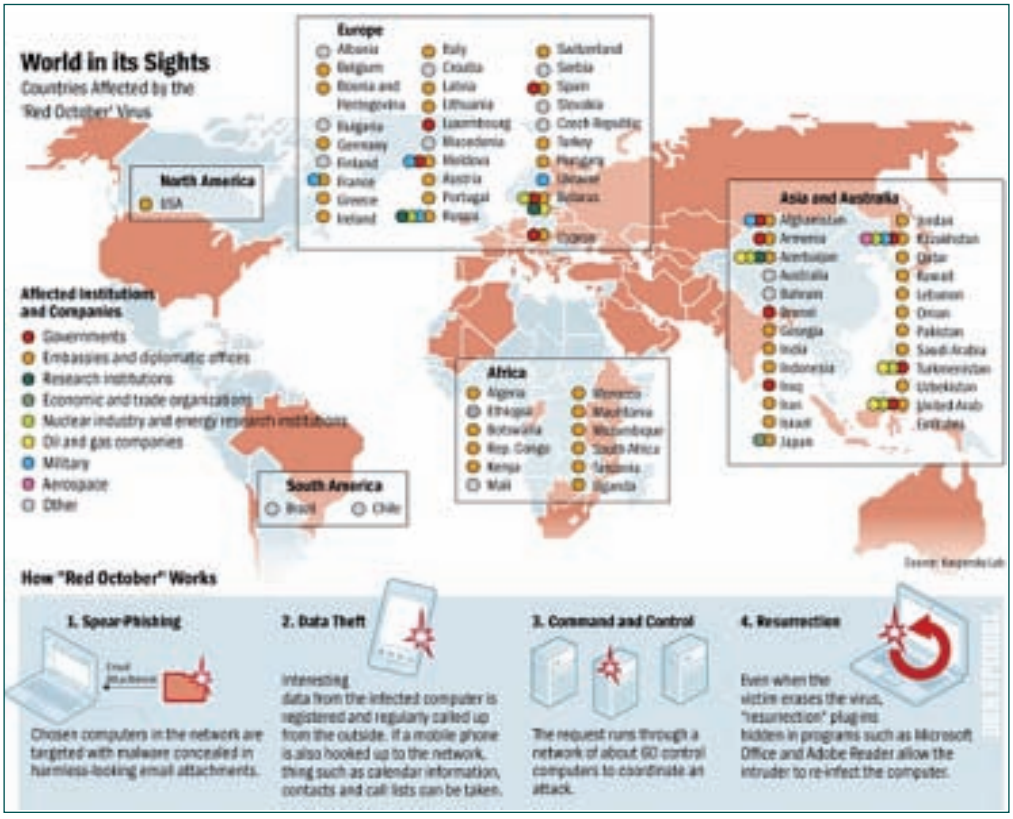

Figura 3. *Paesi colpiti da Ottobre Rosso*
(fonte: www.spiegel.de/international/spiegel/bild-879467-453013.html)

ta delle similitudini con un precedente attacco che risale a luglio del 2011 (figura 3).

In questa 'campagna' di attacchi, denominata da Symantec con il termine 'Nitro', sono circa 48 le aziende che vengono infettate, e sono tutte operanti nel settore della chimica, dei materiali avanzati e della difesa. Symantec identifica in 'Poison Ivy' il *trojan*[23] autore degli attacchi, e attribuisce a hackers cinesi la sua paternità. Ma la Repubblica Popolare Cinese smentisce categoricamente che gli attacchi possano essere partiti da server ubicati nel paese.

Tornando all'*exploit* 'IE zero-day', Symantec conferma in un comunicato[24] che l'utilizzo della vulnerabilità va inquadrato nell'ambito della continuazione del *Progetto Elderwood*. Manifestatosi per la prima volta nel 2009, con attacchi indirizzati contro Google (Operazione Aurora), Elderwood è una piattaforma ricca di *malware* in grado di attaccare bersagli multipli con azioni rivolte all'intrusione nei sistemi e al trafugamento di dati. Gli obiettivi di Elderwood sono stati tutti individuati all'interno della catena di approvvigionamento e servizi del settore della difesa, fino a raggiungere i siti governativi ad essi collegati (figura 4).

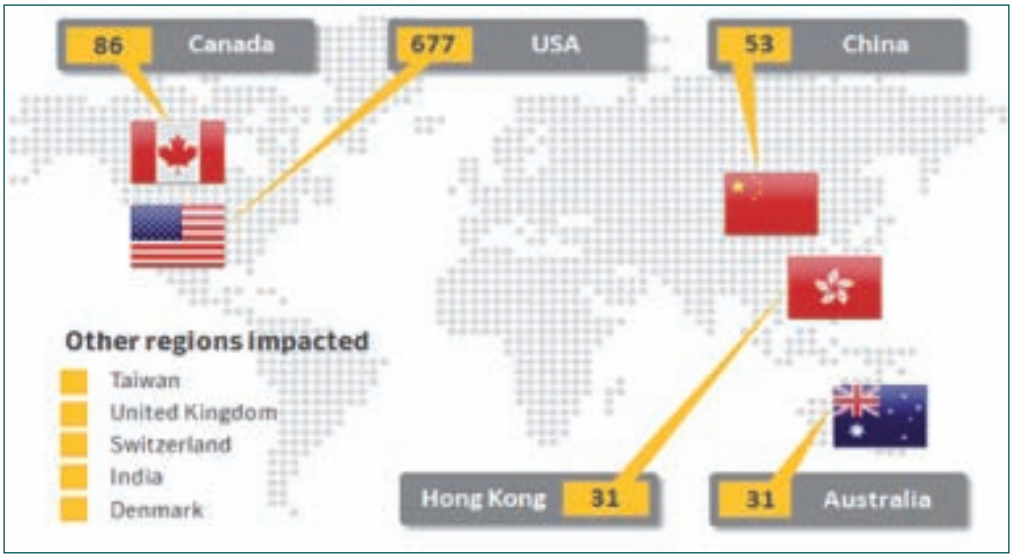

Figura 4. *Numero files utilizzati per gli attacchi effettuati da Elderwood su base mondiale (fonte: www.symantec.com/connect/blogs/elderwood-project)*

23 Trojan. Un *trojan* o *trojan horse* (cavallo di Troia) è un tipo di codice maligno che nasconde le sue funzionalità all'interno di un programma apparentemente utile. Pertanto l'utente che installa un programma apparentemente innocuo e conosciuto, inconsapevolmente, installa ed esegue anche il codice maligno che si annida al suo interno.

24 *www.technewsdaily.com/16217-ie-zero-day-china.html* .

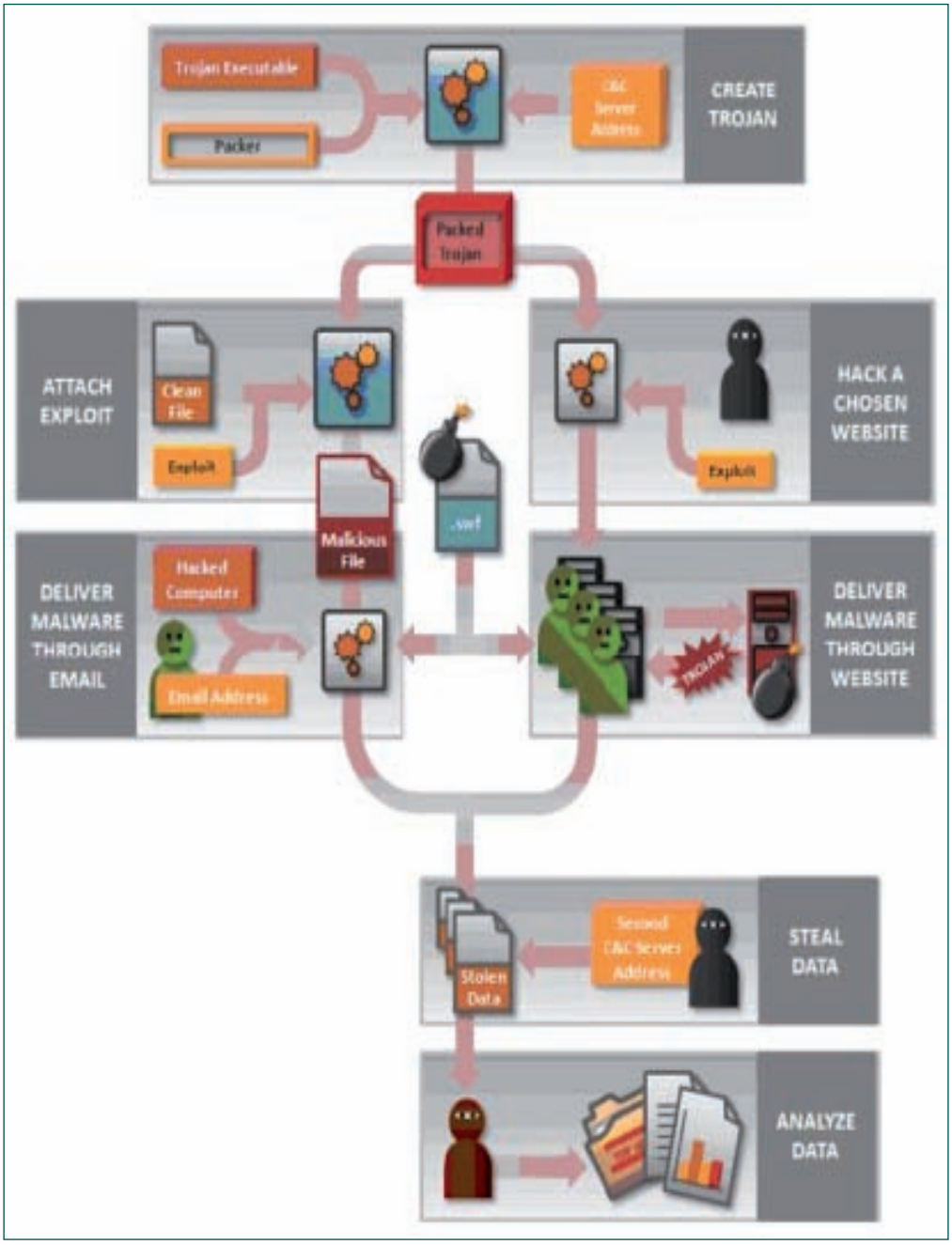

Figura 5. *Funzionamento della piattaforma Elderwood*
(fonte: www.symantec.com/connect/blogs/elderwood-project)

Per quanto concerne gli attacchi, non sono disdegnate le organizzazioni a tutela dei diritti umani e le organizzazioni governative (ONG), che hanno contatti attivi o interazioni con strutture governative e della difesa.

Ma la 'banda' di Elderwood non sembra composta semplicemente da crackers specializzati in tecniche di intrusione nei sistemi, anzi appare come una struttura multiforme in cui si evince la presenza di analisti specializzati nello spionaggio cybernetico, perfettamente consapevoli delle informazioni da ricercare e particolarmente pazienti nel saper attendere il momento più opportuno per lanciare l'attacco.

Dato che il gruppo di Elderwood focalizza l'attenzione sul trafugamento di informazioni 'classificate' o di rilevante valore (forse per un probabile commercio all'ingrosso!), se ne deduce che operano in un contesto di rilevante disponibilità in termini di risorse finanziarie, umane e con altissime competenze professionali. Per una migliore comprensione della tecnica utilizzata, senza tuttavia entrare in tecnicismi che potrebbero essere eccessivamente difficoltosi per i non addetti ai lavori, cercheremo ora di spiegare il funzionamento del sistema Elderwood.

Il suo meccanismo, come si evince dalla figura 5, si basa sulla vulnerabilità *Zero-day*, che si fonda sull'utilizzo di un *exploit* per veicolare un *trojan*. Il codice maligno si introduce all'interno della rete dell'organizzazione e si diffonde rapidamente, raccogliendo, al tempo stesso, tutte le informazioni 'di interesse'. In seguito, i dati 'rubati' sono veicolati su server C&C che si occupano di fornire false indicazioni sui destinatari dei pacchetti dati trafugati (falsificazione dei percorsi di indirizzamento).

In seguito, tutti i dati raccolti sono attentamente analizzati. Un'altra tecnica utilizzata per carpire informazioni, è quella del '*watering hole*' (abbeveratoio). Funziona secondo lo schema collaudato del felino (predatore) che attende le sue vittime in prossimità della pozza d'acqua. L'attaccante cerca di identificare un sito web particolarmente utilizzato dalla sua vittima. Dopo averlo identificato, lo attacca per penetrare le sue difese e iniettare su di esso un codice maligno.

Il virus, che è programmato per identificare la vittima che sta aspettando, rimane in attesa che quest'ultima acceda al sito web. Non appena ciò accade, il virus lo attacca. Pertanto, solo nel momento in cui il malcapitato utente accede al sistema, il virus attiva un meccanismo di penetrazione al suo interno, aggirando i suoi sistemi di difesa. Una volta violato il sistema informatico, si attiva un nuovo trojan che si diffonde in rete tra i computer collegati alla vittima.

Il gruppo di Elderwood ha condotto almeno 678 attacchi contro 216 organizzazioni statunitensi e 86 attacchi indirizzati verso organizzazioni canadesi.

Sono stati attaccati molti sistemi in Australia (31), Regno Unito e India. Ma questa volta non ne è rimasta esclusa la Cina, con ben 53 attacchi identificati, di cui 31 nella sola Hong Kong.

Allora chi si nasconde dietro il progetto Elderwood?
È un paese 'emergente' che sta tentando di sperimentare le proprie capacità tecnologiche o è un'abile manovra di 'intossicazione' delle informazioni sulle vittime del virus?

A febbraio 2013, Eugene Kaspersky, grande patron di Kaspersky Lab, leader europeo nello sviluppo di soluzioni per la sicurezza informatica e la gestione delle minacce, è stato nominato 'Influence of the Year 2012' da Channelnomics[25], per la sua visione e le sue competenze nella sicurezza IT e, forse, anche perché è riuscito a installare le sue applicazioni su un bacino di utenti che può vantare la mitica soglia di 300 milioni. Il suo curriculum, acquisibile dalla Rete, risalta certamente per le lauree conseguite in Crittografia, Telecomunicazioni e Scienze Informatiche ma, forse, anche perché ha conseguito questi titoli di studio in un istituto inglese co-sponsorizzato dal Ministero della Difesa e dal KGB.

Pertanto, non desta particolare stupore che Kaspersky Lab sia tra le poche aziende autorizzate dal Servizio di Sicurezza Federale Russo (FSB) a vendere software di sicurezza antivirus al governo e alle agenzie ad esso strettamente connesse[26].

Non va, inoltre, dimenticato che fu proprio la sua azienda ad analizzare il virus *Stuxnet*, che nel 2010 infettò i sistemi informatici delle centrali nucleari iraniane, bloccandone il funzionamento. Proprio sulla realizzazione di quest'ultimo virus, cui fanno seguito i suoi diretti successori come *Flame* e *Gauss*, aleggia il sospetto della collaborazione tra diverse agenzie di intelligence di governi filoccidentali.

Probabilmente è proprio in funzione di questi timori su possibili alleanze transnazionali nella Cyber Defence, che s'innesta la notizia rilasciata da Strategic Intelligence News[27], in cui si conferma la collaborazione di Kaspersky Lab con il Cremlino per fronteggiare alcuni attacchi provenienti da paesi africani (tra cui il Kenya), ma che in realtà sembrano partire da paesi ostili al governo russo.

A ciò si aggiunge l'ulteriore stranezza che vuole che tra le vittime di Red October vi siano proprio alcuni paesi africani, come Kenya, Uganda, Etiopia, Ciad, Sudan e Eritrea. Fare semplici e lineari congetture nel settore dell'intelligence, può significare giungere a rapide e grossolane deduzioni errate. Non bisogna dimenticare che nell'elenco delle vittime di Ottobre Rosso, la Russia compare esattamente ai primi posti!

Come evidenziato in figura 2, risulta chiaro che alcuni paesi del sud-est asiatico (tra cui la Cina), non sono stati 'attenzionati' da Ottobre Rosso.

Ma è, altresì, vero che neanche i sistemi informatici che risiedono in altri paesi, come il Canada o il Messico, sono stati oggetto di attacchi.

25 *http://channelnomics.com/* .

26 *http://mytech.panorama.it/kaspersky-putin-spie-kgb-pussy-riot* .

27 *http://intelligencebriefs.com/?p=3308* .

Alla luce di tutto questo il Presidente Barack Obama, il 12 febbraio scorso, ha deciso di siglare un nuovo ordine esecutivo[28] per rafforzare la sicurezza informatica a livello nazionale.

L'obiettivo è di fare in modo che le aziende statunitensi, e in particolare quelle di rilevanza strategica, condividano una serie di informazioni, prodotte dalle agenzie federali, sulle recenti possibili minacce informatiche e i rischi derivanti dall'utilizzo delle tecnologie digitali.

Il programma Enhanced Cybersecurity Services sarà esteso anche alle società che operano nel settore delle infrastrutture digitali, per ampliare le azioni di contrasto al cyber-crime.

Nulla è ciò che sembra!

È forse la regola più antica del settore dell'intelligence: nulla è ciò che sembra. Probabilmente proprio su questa regola si potrebbe basare un'analisi più attenta sulle possibili origini di Ottobre Rosso. Gli eventi, le informazioni, le news che quotidianamente ci assalgono e contribuiscono a riempire quel contenitore informativo che dovrebbe trasformarsi in conoscenza individuale, spesso invece contribuisce ad accrescere quella confusione mentale (overload informativo) che ci conduce verso considerazioni e conclusioni completamente errate. Ed anche in questo caso, le informazioni di cui disponiamo potrebbero rivelarsi incomplete, distorte o opportunamente manipolate per indurci a convincimenti sbagliati.

Proviamo ad inserire un nuovo elemento di analisi.

A giugno del 2012, secondo quanto riportato da Space Daily[29], il governo della Corea del Nord viene accusato da quello del Sud di aver attivato un 'élite team' di hackers capaci di trafugare segreti militari per fomentare il disordine pubblico all'interno del governo di Seoul. '*La Corea del Nord sta cercando di rubare segreti militari e paralizzare il nostro sistema di difesa e informazioni utilizzando esperti appositamente addestrati per incidere nella nostra rete di informazioni militari*' questo è quanto asserisce il Defence Security Commander del governo di Seoul, Bae Deuk-Shik in un convegno sulla sicurezza, aggiungendo poi che il Nord ha tentato di '*fomentare il disordine sociale, di paralizzare la nostra infrastruttura di base attraverso il cyber-terrorismo che può causare enormi danni in un breve periodo*'.

Il professor Lee Dong-Hun della Korea University ha confermato, durante il forum, che il governo di Pyongyang ha istituito anch'essa una 'special unit' forte di circa 3.000 *hackers*, controllati e diretti dallo stesso leader del paese, Kim Jong-Un.

[28] *www.corrierecomunicazioni.it/it-world/19607_obama-vs-cybercrime-ordine-esecutivo-sull-it-security* .

[29] *www.spacedaily.com/reports/S_Korea_military_accuses_North_of_stealing_secrets_999.html* .

Ma il professore si è spinto ben oltre, affermando perfino che la '*Corea del Nord è la terza nazione più potente al mondo nella cyber-guerra, dopo Russia e Stati Uniti*'.

Sembrerebbe, quindi, che la Cina, con le sue potenzialità economiche, scientifiche ed infrastrutturali, sia inferiore alla Corea del Nord, per quanto concerne le strutture, le tecnologie e le professionalità dedicate alla cyber-war.

Secondo quanto pubblicizzato sui media internazionali, dal 2009 e fino al 2012, molti siti sudcoreani con una particolare attenzione rivolta a quelli che afferiscono al settore finanziario (banche), sono stati attaccati da malware di tipo DDoS[30], grazie alla cooperazione di studenti universitari reclutati nelle università della Corea del Nord.

Ovviamente Pyongyang accusa Seoul di inventare le accuse. Nello stesso anno, tra aprile e maggio, Seoul ha nuovamente accusato la Corea del Nord di aver utilizzato segnali radio per azioni di *jamming* (azioni di disturbo delle comunicazioni radio).

Sembra, però, corrispondere al vero la notizia che, già da alcuni anni, sia operativo un nucleo di 'élite crackers' specializzati in cyberware, cui si aggiungerebbe l'ulteriore collaborazione di circa 10.000 laureati in aree tecnico-scientifiche che provengono dalla Kim Il Sung University. La struttura di 'élite' si troverebbe all'interno della 'Room 39' (conosciuta anche come Bureau 39, Division 39 e Office 39), un'organizzazione segretissima alle dirette dipendenze del governo di Pyongyang, specializzatasi soprattutto in audaci e spericolate operazioni finanziarie sui mercati internazionali. Sembra, addirittura, che questa struttura, alle dirette dipendenze di Kim Jong-Un, si occupi di molteplici attività riservate tra cui il programma di sviluppo di armi nucleari. Tuttavia, il ben noto isolamento in cui versa la Corea del Nord, impedisce quasi totalmente l'accertamento di queste informazioni. Va sottolineato che la Corea del Nord è un altro di quei paesi usciti indenni dagli attacchi di Ottobre Rosso.

In funzione di ciò si potrebbero elaborare facili congetture sulla paternità di Ottobre Rosso, ma se osserviamo bene gli ambienti geografici in cui si sono consumati gli attacchi, possiamo rilevare che sono stati esclusi dai cyber-attack anche molti paesi collocati geograficamente in un altro continente.

È il caso dei paesi africani, che potrebbero essere considerati come 'out of technology', per la loro proverbiale arretratezza tecnologica e cronica scarsità di mezzi, ma anche in questo caso si rischia di commettere un grossolano errore di valutazione delle effettive potenzialità possedute. Al contrario di quanto si possa immaginare, da qualche tempo, molti paesi africani hanno iniziato ad organizzarsi per un loro ingresso, e soprattutto 'ruolo', nel Cyberspazio.

[30] DDoS (Distributed Denial of Service). In informatica, un DoS (Denial of Service) corrisponde ad un attacco informatico che mira alla negazione di un servizio. Il funzionamento si basa sul tentativo di disattivare un servizio offerto da un sistema informatico (ad esempio un sito web). Una variante di questo tipo di attacco è il DDoS che, funzionando allo stesso modo, tenta però di condurre l'attacco utilizzando numerosi computer attaccanti, che insieme costituiscono una botnet.

Già da diversi anni, in molti di quei paesi considerati 'caldi' (dal Medio Oriente all'Africa), dove gli investimenti erano perlopiù concentrati sull'acquisto di armamenti e tecnologie militari, si sta cominciando ad inserire una nuova voce nel bilancio della spesa nazionale: la Cyber Defence.

Gli esempi non mancano: il Kenya ha annunciato[31] che assegnerà ad ogni utilizzatore della Rete, un'identità virtuale per arginare il crescente fenomeno del cyber crime. Ma Bitange Ndemo, segretario permanente del Ministro delle Informazioni e Comunicazioni del Kenya, ha asserito '*Ci stiamo muovendo velocemente verso l'automazione di tutte le informazioni, dato che i sistemi informativi devono essere protetti perché alcune persone hanno cattive intenzioni*'.

E l'ha detto proprio in occasione dell'East African Cyber Security Convention del 2012, evento sulla sicurezza informatica cui hanno partecipato, con nutrito interesse, quasi tutti i paesi del continente africano. Ndemo ha anche asserito che, in seguito ai numerosi attacchi informatici subiti nel corso degli ultimi mesi contro banche e aziende di comunicazione e trasmissione dati, sta realizzando un ecosistema di cyber security all'interno della Communication Commission of Kenya (CCK) che ha la mission di contrastare le minacce informatiche provenienti dal Cyberspazio. Ma ciò che non bisognerebbe mai dimenticare è che una struttura di Cyber Defence può tranquillamente svolgere azioni di Cyber Intelligence.

Molti pensano che la strada migliore per affrontare il problema della Cyber Defence, sia quella della collaborazione transnazionale. Ed è proprio su questo convincimento che dal 2011 Stati Uniti ed Unione Europea stanno sperimentando la via della cyber-sicurezza congiunta. Una prima esperienza è consistita nella realizzazione dell'esercitazione 'Cyber Atlantic 2011', che ha visto la collaborazione dell'ente europeo ENISA (European Network and Information Security Agency) e dello US Department of Homeland Security.

Complessivamente sono stati 20 i paesi coinvolti in simulazioni di cyberattacchi, gestione di scenari di crisi da attacchi provenienti dalla Rete su infrastrutture critiche, furto di dati da sistemi informatici, attacchi a infrastrutture energetiche.

Altri paesi sono, invece, convinti del contrario e, cioè, che la condivisione di risorse tecnologiche e delle competenze, possa risultare 'poco conveniente' in un mondo intrinsecamente instabile, in cui anche le più solide collaborazioni o gli storici legami di amicizia, possano venir meno per sopraggiunte esigenze legate ai continui mutamenti che si verificano nel mondo a livello economico, politico e sociale.

In conclusione, dietro Ottobre Rosso potrebbero celarsi forze oscure non meglio identificate o più semplicemente azioni sinergiche di più paesi interes-

31 *www.businessdailyafrica.com/Corporate-News/-/539550/1624124/-/yi8poj/-/index.html .*

sati al trafugamento di informazioni, vitali per la loro sopravvivenza, in un mondo governato dalla 'globalizzazione socio-economico-produttiva'.

L'informazione è potere, e per assumere una posizione di rilievo a livello mondiale è essenziale l'acquisizione continua di informazioni, cui deve affiancarsi il diretto controllo delle stesse.

Ma, essendo l'informazione sempre più digitalizzata, bisogna munirsi di strumenti e risorse umane che siano in grado di intercettarla dove è prodotta e acquisita: il *Cyberspazio*.

Bibliografia

http://www.spiegel.de/international/spiegel/how-russian-virus-hunters-tracked-down-a-global-espionage-network-a-879467.html

http://www.matthewaid.com/post/42178624483/red-october-spyware-system-used-sophisticated

http://www.csmonitor.com/USA/2013/0115/Digital-fingerprints-on-Red-October-spyware-point-to-Russia-or-do-they/(page)/2

http://www.technewsdaily.com/16373-red-october-spyware.html

http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies

http://arstechnica.com/security/2013/01/why-red-october-malware-is-the-swiss-army-knife-of-espionage