Citizen Lab, Munk School of Global Affairs, University of Toronto

MUNK SCHOOL OF GLOBAL AFFAIRS

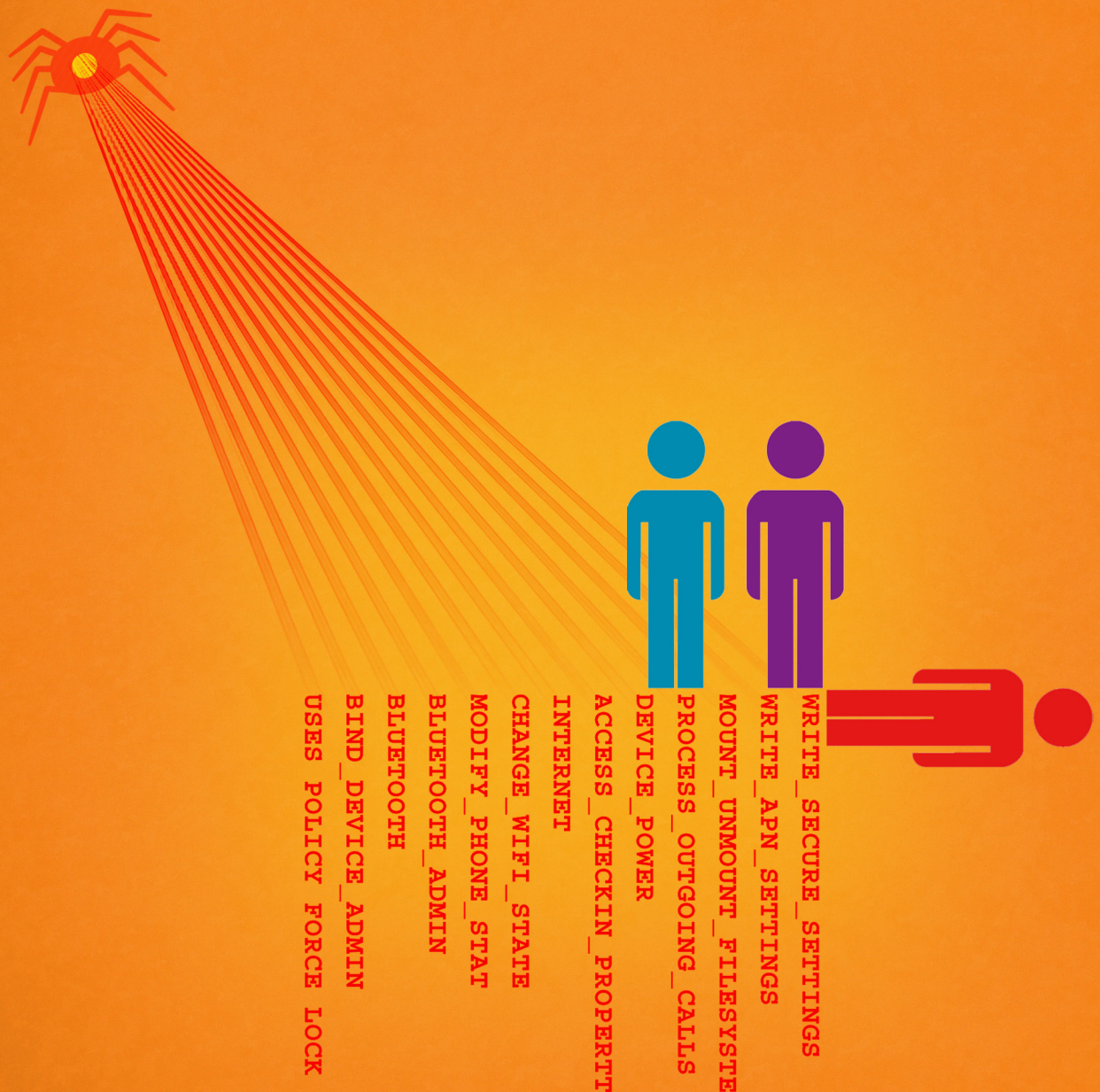
UNIVERSITY OF TORONTO

COMMUNITIES @ RISK

Targeted Digital Threats Against Civil Society

November 11, 2014

https://targetedthreats.net/



GLOSSARY

Technical Glossary

ActiveX

A software framework created by Microsoft that allows for embedded objects such as scripts, images, movies, or programs to be added into other document types, like web pages. Malicious ActiveX controls are often used by attackers to gain unauthorized access to computer systems.

Advanced Persistent Threat (APT)

Advanced persistent threat (APT) is a term used to describe digital attacks that compromise computer systems with the intent of collecting data and monitoring communications without being noticed. They typically intend to persist for months or even years, and are generally associated with harvesting of information for political or economic purposes. The term is not to be confused with 'APT1', the name given to a specific threat actor group.

Android Application Package (APK)

A file format that is used to distribute software for the Android platform of mobile devices.

Antivirus (AV)

A class of applications that seek to identify malicious software, often by using a library of signatures previously identified as being associated with malicious software.

Attack Vector

The entry point by which an attacker gains unauthorized access to a computer system. Examples of an attack vector would be a malicious email attachment, sending a malicious link, or sending malicious files through an instant messaging program.

Backdoor

A method by which an attacker maintains access and control of a system after an initial compromise. This could be in the form of a hidden server listening on a port for an attacker to connect.

Beaconing

In terms of malicious network traffic, beaconing is a network pattern whereby malware

sends out network traffic to a command and control server (C2) at regular intervals. Beaconing traffic can serve as a "heartbeat" signal to inform the command and control server that a given client is active.

Botnet

A distinct network of machines, typically compromised by malware, that is controlled by attackers without the permission or knowledge of their owner.

Campaign

Campaigns are collections of targeted malware attacks that share some common infrastructure or resource. Targeted malware attacks are typically not one-off events, and in many cases malware samples can be grouped together as "campaigns" based on common C2 infrastructure, malware development, social engineering tactics, or static analysis of malware code.

Cluster

A grouping of malware samples that share common features. Examples of these commonalities include shared command and control infrastructure, shared originating IP address, shared tactics, or shared malware development branches.

Collateral Compromise

A computer compromise that results in the additional or unintended compromise of additional targets. An example would be the compromise of clients that use shared web hosting, when the intended attack target is just one client of many hosted on a given server.

Command-and-Control (C2)

Command-and-control ('C2' or 'C&C') servers are computers used to send and receive commands and data to computers infected with malware. Upon being infected with malware, a compromised computer will attempt to contact a C2, which issues it commands, sends additional malware to install and exfiltrates data. C2 infrastructure can take different forms, with the most common being a domain name either registered or compromised specifically to act as a C2. It is often possible to link different malware attacks together through their use of common C2 infrastructure.

Common Vulnerabilities and Exposures (CVEs)

A dictionary of common names for publicly known security vulnerabilities. CVEs are composed of the format: CVE-YYYY-NNNN, where YYYY references the year of discovery and NNNN references a unique number for the CVE. CVEs are commonly used to establish a common language when discussing security vulnerabilities.

Distributed Denial of Service (DDoS)

A type of attack in which a service is flooded with simultaneous requests in an effort to render a service unstable or unusable. When these requests are made with multiple computers or even botnets these type of attacks are considered "distributed"

Dynamic-Link Library (DLL)

A file used by other programs instead of directly by the user. They often contain features that are optional, or shared with multiple programs.

DLL Hijacking

DLL Hijacking is the technique of using a legitimate program with a malicious shared library that shares the name of a system library. Some programs, if not configured properly, will look for the shared library by name, with priority going to a library with that name in the current path. This allows an attacker to add malicious code to a program without modifying its valid digital signature.

Defacement (website)

A website defacement is a malicious act that replaces the contents of a website with content written by an attacker that has gained unauthorized access to a website. These messages can vary in content from lewd content to political statements.

Domain Name Service (DNS)

An Internet service analogous to a phone book that translates human friendly and easy-to-remember domain names to IP addresses. For example DNS translates domain.com into the IP address 65.254.244.180.

Dynamic Domain Name Service (DDNS)

A method of updating a DNS record in situations where the IP of a client can change, such as a home Internet connection. DDNS domains are often composed of two sub-domains in the format {given_name}.{ddnsprovider}.com Free DDNS services are often favored by attackers for command and control domains as they do not require a user to provide proof of identity or payment where regular domain services do.

Drive-by Download

An unintended download of a file that is the result of simply visiting a malicious or compromised web page.

Drop

Any file that is created during the execution of malicious software.

Exfiltration

Exfiltration is the process of collecting data (such as documents, emails, contact lists, or even microphone or webcam data) from a compromised computer or device and

sending it back to the attacker. Attackers will traditionally encrypt and compress data before exfiltration.

Exploit

A piece of computer code that takes advantage of a flaw or glitch in software in order to cause a result that is either unexpected, unintended or malicious. Exploits are commonly used by attackers to gain unauthorized access to computer systems.

Flag Text

Flag text refers to a defining piece of text that is present in malicious network traffic (often a preamble) that ties it into a specific family or type of malware. For instance the Gh0st RAT family of malware will commonly use Gh0st as the flag text in its network traffic.

Hash

A hash is a string of hexadecimal characters that identifies a file; should the file change in any way, the hash will as well. Hashes are designed to be easy to compute from a file, enable checking to ensure that the file has not been changed, and to compare files to determine if they are identical.

Header (email)

A group of field/value pairs that precede email messages that describe routing information as well as meta data, and path information for emails. In computer security, email headers are valuable in determining spoofed senders and other anomalies in messages.

Header (file)

A file header refers to additional information, commonly metadata, that is placed at the start of a file or a block of data.

Infrastructure

In terms of computer security, infrastructure, refers to the totality of an attackers computer resources. Computer servers that are used for malicious means as as well as IP addresses and compromised machines make up parts in a given attacking infrastructure.

Java

A programming language whose code must be executed through a virtual machine that is typically installed as a software package. Java programs are distributed as Java ARchive files (JARs). Flaws in how Java handles certain code are often exploited by attackers to compromise computer systems.

MD5

MD5 hashes, also called message digests, are often used to identify a file based on

its content. MD5s take the form of a string of hexadecimal data, such as '6fb3ecc3d-b624a4912ddbd2d565c4395'. If two files have the same hash, they are the same file. MD5s are frequently used to compare samples of malware from different sources to identify if they are the same.

Malware

Also known as malicious software, refers to software that is installed on a computer, often by deceit or trickery, that serves to disrupt operation, or gain unauthorized access to a given computer or its files.

Malware Family

A broad grouping of malicious software that share common features or development branch. Examples of malware families include ShadowNet, sparksrv or PlugX.

MIME HTML (MHTML)

An archive web page format that is used to wrap HTML code and associated files such as images, and scripts into a single file. This is commonly used in creating format rich e-mail messages. Attackers outlined in this report commonly exploit how these files are handled in Microsoft Word in order to compromise computer systems.

Mutex

Short for 'mutual exclusion', mutex is a process to prevent multiple threads of a program from accessing the same data at the same time.

Network Intrusion Detection System (NIDS)

A network appliance that the examines network traffic of a computer or network in order to detect patterns that are indicators of attack, compromise, or suspicion of either.

Obfuscation

Any attempt to hide the content or intent of a communication or a piece of data. Obfuscation is sometimes used by malware to hide the fact that it is malicious, or to make analysis more technically difficult or resource intensive.

Packet Capture (PCAP)

A file format that includes the totality of network traffic, including headers and payloads, for a given period of time, or based on particular criteria.

Passive DNS

An information service that records the results of DNS queries passively over a long period of time in order to track the historical values of DNS lookups.

Payload

The portion of a network transmission that is the intended purpose of that transmission.

For instance, if someone is logging into a website, the username and the password that is sent is a payload while any network headers or meta data are not. In computer security a payload refers to the portion of a file that performs the malicious action.

Remote Access Trojan (RAT)

A remote access trojan (RAT) is a software tool that allows a user to remotely access and control another computer. While remotely controlling a computer is a common and legitimate form of system administration, the term 'RAT' is used to refer to surreptitious and illegitimate access to a remote computer. While the sophistication of RATs can vary, they often have a similar set of capabilities, such as the ability to exfiltrate data, take screen captures, enable webcams/microphones, and install additional software.

Rich Text Format (RTF)

A file format developed by Microsoft intended for text documents with a modest amount of formatting information. Exploits in how Microsoft Word handles this format are commonly used by the attackers outlined in this report.

Social Engineering

Deceiving an intended target of compromise by non technical means such as trickery, flattery, or appeal to authority. The composition of e-mail messages where there is a malicious attachment is a common form of social engineering.

Spearphishing

Spearphishing is a term to described the use of targeted email attacks designed to compromise a specific individual or group. Spearphishing is a more targeted form of phishing (attacks sent to a broader group of targets).

Spoofing (email)

A spoofed email is a technique whereby the original sender of a message is masked or outwardly replaced. This is typically used to deceive the recipient and assist in social engineering.

Spyware

A piece of software that gathers and sends information about the computer it is installed by without the owner's consent or knowledge. Spyware ranges from web browser tracking cookies to expertly designed malicious programs.

Stage 0 / Stage 1 / Stage 2 / etc.

The staging system outlines the phases by which malware evolves and expands on a compromised computer system. Stage 0 refers to the initially received malicious file. Stage 1 refers to the malicious payload of that file. Stage 2 refers to any additional files that the payload may download from an external source once executed. Additional

stage numbers are used if the file downloads still more components.

The Onion Router (Tor)

An encrypted network service designed for anonymity and circumvention of Internet censorship. Tor is sometimes used by attackers to hide their true location of either themselves or command-and-control servers.

Trojan

A type of malware program that masquerades as another type of file but actually causes a computer system harm, like installing a backdoor or stealing user information.

Unicode Right-to-Left (RTL) Override

Unicode is a system for encoding and display of characters on a computer. There are currently over 110,000 characters that can be displayed with Unicode. Some Unicode characters have special meanings that alter the way text is displayed, instead of representing a specific character. The Unicode Right-to-Left (RTL) Override is an invisible character that, when displayed, changes the direction of text flow to the left. This is often used as a trick to hide the true extension of a file by displaying a file name backwards.

User Account Control (UAC)

A security feature of Microsoft Windows. Introduced in Windows Vista and Server 2008, this feature aimed to improve security by employing a more strict separation of user privileges. Properly implemented user privilege separation can make the execution of malware more difficult.

Virtual Private Network (VPN)

A method by which private computer networks can communicate through public networks. A commonly used VPN configuration, for example, allows remote employees to communicate with the computer network of their company. Malicious attackers sometimes use VPNs as a portion of their attack infrastructure.

Virtual Private Server (VPS)

A virtualized computer server that is sold by a company, often for the purposes of hosting a website or publicly accessible Internet service.

VirusTotal (VT)

A free service owned by Google Inc. that allows users to submit samples of suspicious files in order to be scanned by a variety of antivirus engines. These samples are made available to subscribers in the security community.

YARA signatures

YARA is a software tool used by malware researchers to identify and classify malware

samples. Each sample is given a signature, which lists identifying features of the malware. As part of this project, we have created YARA signatures for the malware we have identified.

Watering Hole Attack

A type of targeted attack in which a malicious actor compromises a website that is commonly visited by their intended victim(s). It is named a watering hole attack because the attacker seeks to attack or poison a commonly visited area (the watering hole) as a means to attack a certain group.

Windows Management Instrumentation (WMI)

A Windows abstraction layer that exposes information and notifications about software or hardware often for the purposes of system management software or system administration scripts. Attackers can write malicious WMI scripts in order to make malware more difficult to identify in cases of compromise.

XOR

XOR is the "exclusive or" logical operation. This operation is commonly used in cryptography although XOR alone is considered a very weak form of encryption. XOR encryption is sometimes used as a very basic method by which malware protects data such as the command and control server it uses.

Zero-day

Also known as "0day" is an attack that exploits a previously undocumented or unreleased flaw in software. Zero-day attacks are significant because they are difficult to discover (and hence costly for attackers to acquire and use) and difficult to defend against.