MULTI-STATE Information Sharing & Analysis Center™

INTEL PAPER

Common Cyber Threats to Universities

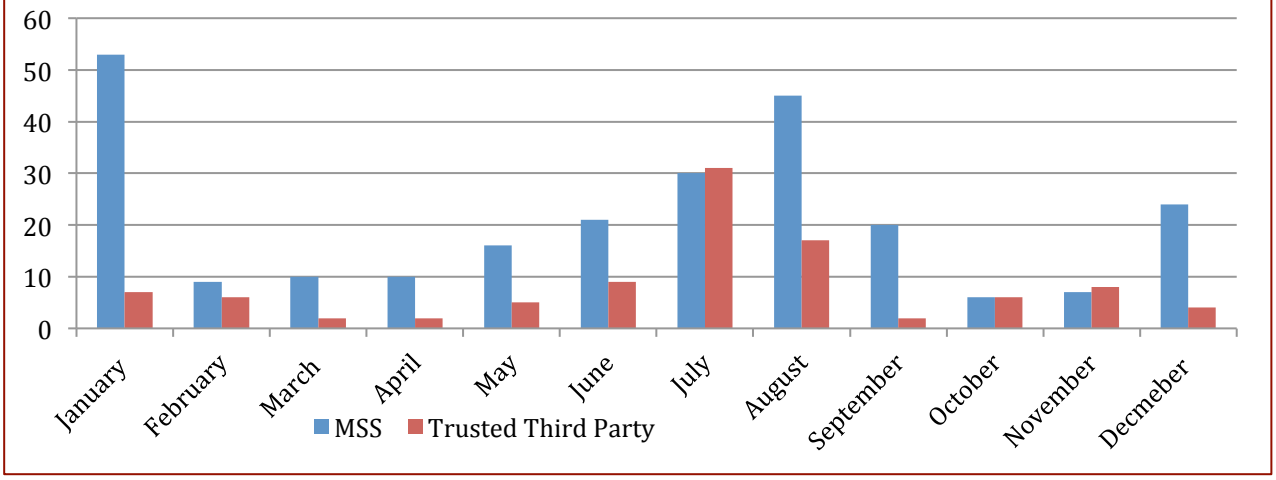
February 23, 2016, IP2016-0113

Risk: ***High*** *probability of occurrence – Impact:* ***potential high*** *impact event*

(U//FOUO) TLP: **AMBER** **The Risk:** The Multi-State Information Sharing and Analysis Center[U.S. entity] (MS-ISAC) assesses with high confidence that cyber threat actors routinely target universities, for the purposes of financial gain, notoriety, or entertainment, and often to gain access to personally identifiable information (PII) and/or sensitive research. MS-ISAC believes universities are inherently more vulnerable to cyber targeting than other state, local, tribal, and territorial (SLTT) government entities, due to the non-restrictive research environment with less compartmentalization and less access restriction, which results in more opportunity for infection, and when infection occurs, easier transmission through a network.

- Incident frequency remained relatively consistent in 2015 compared to 2014, but incidents spiked in July and August 2015 as seen in Figure 1. The August spike may be partially caused by the return of students to campus and increased traffic on university networks.
- Nation-state actors pose the gravest threat to universities systems and the greater national security interest. This is due to nation-state actor's more advanced skill sets and tendency to strategically target universities with developed research programs, or those that are Cleared Defense Contractors (CDC) or Centers for Academic Excellence (CAE), which may contain engineering, health, science or defense research, crucial to the U.S. National Security interest.
- Based on MS-ISAC data, universities are most likely to be targeted via a phishing email, and malware infection is the most likely tactic, technique or procedure (TTP) a university will experience.

University Events Detected by MS-ISAC Montitoring Services in 2015 **Figure 1**



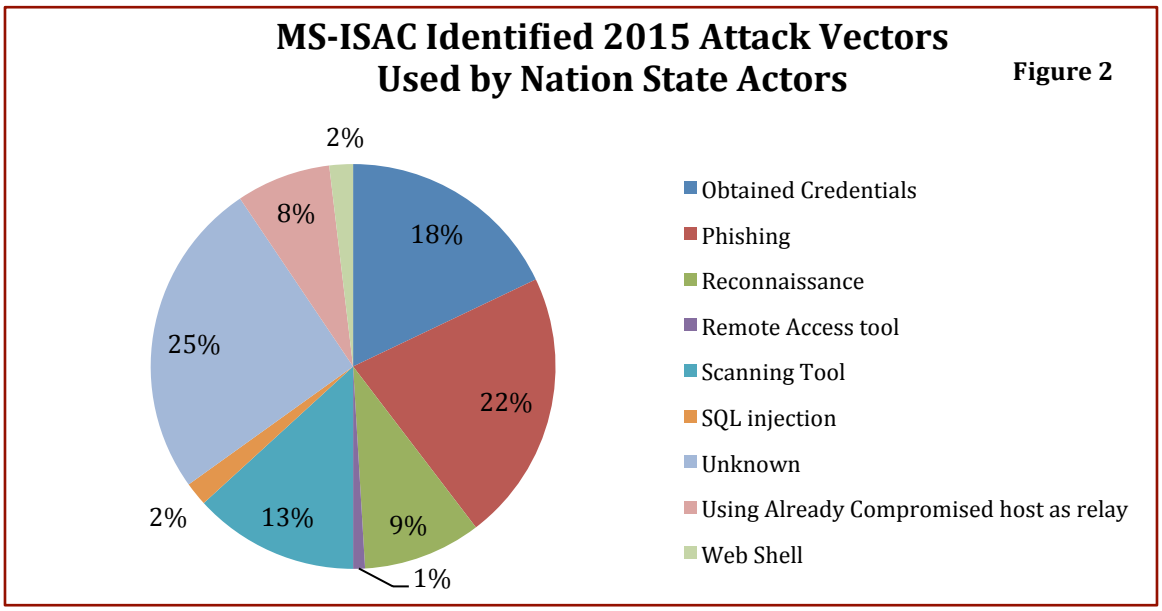
(U//FOUO) TLP: **AMBER** **Cyber Threat Actors:** MS-ISAC determined four groups of malicious cyber threat actors frequently involved in targeting universities: nation-state actors, hacktivists, financially-motivated cyber criminals, and student insiders. Additionally, there are incidents not associated with any actor.

- *Nation-state actors* pose the gravest threat to the United State's national security interests, as they aggressively target and gain persistent access to public and private sector entities, including universities, to compromise, steal, change, or destroy information. They are also commonly referred to as Computer Network Exploitation (CNE) operators and Advanced Persistent Threats (APT). Based on MS-ISAC information, we believe that nation-state actors primarily target universities with esteemed research programs, as well as universities that are CDCs, and CAE's. The main method of compromise is phishing emails, and common TTPs involve downloading malware and elevating privileges to enable further malicious activity.

(U//FOUO) TLP: **AMBER** *Although nation-state actors frequently use hop points, which decreases our confidence in this assessment, MS-ISAC believes nation-state activity originates most frequently from China, Russia, and the middle east.*

MS-ISAC Identified 2015 Attack Vectors Used by Nation State Actors

Figure 2



- *Hacktivists* are politically, socially, or ideologically motivated, and target victims for publicity or to effect change. This group poses a low to moderate threat to the overall operations of a university, but universities are likely to experience hacktivist related incidents over the course of a year. Hacktivists target universities with both opportunistic and strategic attacks, and according to MS-ISAC data, most commonly execute website defacements and printer defacements, but occasionally conduct DDoS attacks and SQLi attacks.
- *Cyber Criminals* are largely motivated by profit, and almost always seek to obtain data that has a financial value, such as PII, or gain access to sources of valuable data, such as vulnerable Point of Sale (POS) systems at university cafes and stores. They are occasionally motivated by a desire to build a reputation.
- *Students as the attacker*: Universities also face an insider threat from the students themselves. There are recorded incidents of students attacking a university system to prove a point about vulnerable systems, change grades, or pull pranks through website defacements.

(U//FOUO) TLP: **AMBER** **Targets:** While university targeting often occurs *opportunistically*, analysis of the victim universities revealed patterns that suggest certain malicious cyber threat actors also *strategically* target them. Most of the strategic targeting can be attributed to nation-state actors and involves universities that are CDCs and/or CAEs, and/or universities with strong science, technology, engineering, and math (STEM) programs.

(U//FOUO) TLP: **AMBER**
Occasionally, students strategically target their own schools or rival schools with malicious cyber activity. However, this is extremely rare.

- CDCs are entities that have been granted clearance by the DOD to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of a Department of Defense program.
- CAEs are National Security Agency[U.S. entity] (NSA) and Department of Homeland Security[U.S. entity] (DHS) recognized universities that meet academic criteria for cybersecurity education.
- Targeted STEM programs include physics laboratories, biological science departments, computing centers, environmental studies centers, medical centers, robotics departments, and other similar programs.

(U//FOUO) TLP: **AMBER** *While the data suggests that the types of universities listed above are strategically targeted, it is also possible that these departments monitor their systems more diligently than other departments and/or are more diligent about reporting compromises, which would result in a data bias.*

(U//FOUO) TLP: **AMBER** **Attack Vectors:** MS-ISAC assesses with high confidence that the most common attack vectors used by malicious actors to compromise university systems are phishing emails followed by Structures Query Language injection (SQLi) attacks, brute force attacks, web shells, and drive-by downloads.

- *Phishing* is the most popular method used by cyber threat actors to compromise university systems and networks. Universities are particularly susceptible to phishing attacks because of the readily available information about faculty, staff, and students, which can assist in social engineering, as well as the open sharing environment. For example, cyber threat actors may craft an email that identifies them as a student or colleague interested in a professor's research and attach a "paper they would like reviewed," which actually downloads malware when opened. Alternatively, they may solicit information by offering a presentation or employment opportunity.
- *SQLi attacks* are the second most common method of compromise used to target university systems and networks. Cyber threat actors use this attack to exploit the relationship between a web application and a database by typing a SQL command into a web form field in an attempt to access the information stored in the database. If the SQLi vulnerability is successfully exploited, the actor could view, exfiltrate, modify, delete, or corrupt the information. SQLi attacks against universities often result in a breach of systems containing PII, which malicious actors publish to posting sites or sell.
- *Brute force attacks* are a trial and error method used to obtain login credentials or a personal identification number to gain access into a system. This method often utilizes automated software to generate a large number of consecutive guesses. MS-ISAC observed cyber threat actors using this method multiple times on university systems.

- *Web shells* involve uploading a program or script onto a vulnerable website or server, allowing an unauthorized user to execute commands and potentially access information hosted on that server. This technique has been used on university websites to download malware, conduct web defacements and data breaches, and other malicious activities.
- *Drive-by downloads* are a likely vector for malware infections on a university system. Drive-by downloads occur when a user visits a website that then downloads malware on to the computer, often without needing any other approval or action on the part of the user. Universities are often victimized by drive by downloads, but could also be unknowingly hosting a website facilitating drive-by-downloads, if compromised.

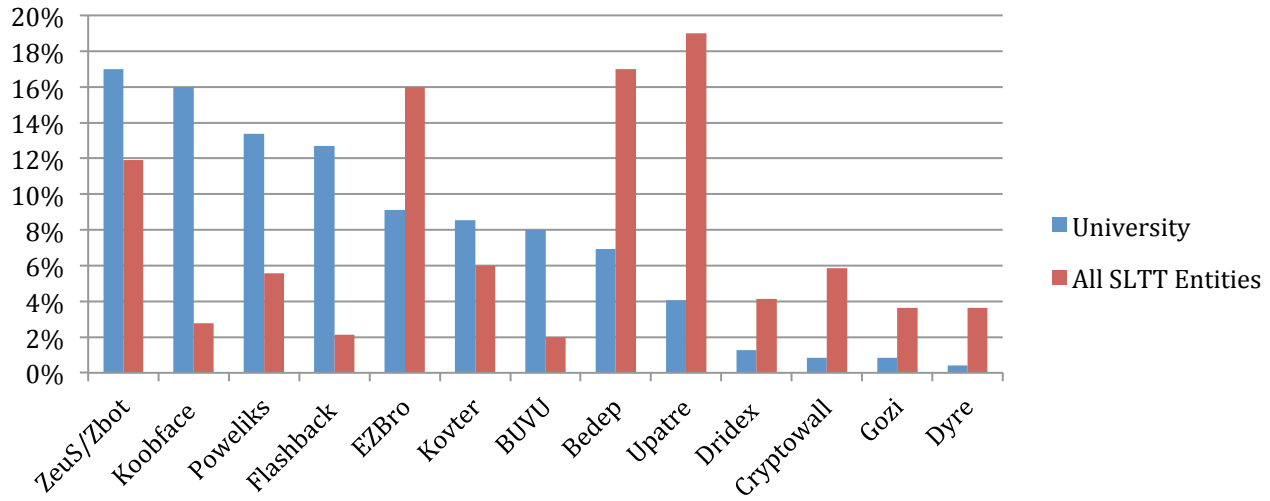
(U) TLP: **AMBER** Case Study: A public university became the victim of a nation-state related attack when the nation-state operators used social engineering to target employees who worked with China. The operators were then able to move laterally through the network and gain access to additional university systems.

(U) TLP: **AMBER** Case Study: Netflow analysis of one public university's outbound traffic logs that a network account engaging with a Russian IP address and the exfiltration of large amounts of information. Contact with the university confirmed that a "suspicious" user account was created and responsible for the traffic.

(U//FOUO) TLP: **AMBER** **Tactics, Techniques, and Procedures:** Cyber threat actors use a wide variety of TTPs on universities, which are very similar to the TTPs observed in use against other SLTT government entities. Malware infections are the most common of these, followed by web defacements, account compromises, data breaches, DDoS attacks, the use of hop points, and scanning and reconnaissance.

- *Malware* infections are one of the most common cyber TTPs that affect university systems. Analysis of malware infections revealed that malware trends for universities are different than the malware trends across all other SLTT entities (Figure 3). This discrepancy in malware is likely caused by the non-restrictive research environment prevalent at universities, combined with the predominately younger demographic on the network.

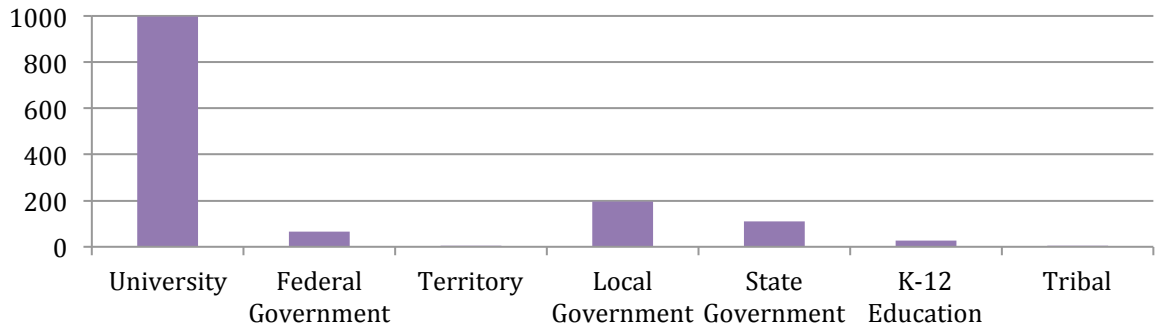
Figure 3



  - For example, Koobface, a network worm that infects users of social media platforms such as Facebook, is the second most popular infection type on university systems, but is much less common among other SLTT government entities. This is most likely because universities do not restrict Facebook access, whereas many other SLTT government entities may restrict access.
  - Other noteworthy discrepancies observed include the percentage of flashback malware observed on universities verses other SLTT entities. Flashback, a malware that only effects MACs, is likely more prevalent on university systems because MAC operating systems are more popular in universities than in other SLTT government entities.
- *Account Compromises* affect universities when a malicious actor obtains usernames or email addresses, and passwords from a compromised database, and posts this information to a pasting website. These exposed credentials could lead to a university compromise if a cyber threat actor utilized the posted credentials to obtain access to a university network. University account information is commonly compromised when external databases are compromised and the data is posted online.
- *Web server defacements* are low-level compromises most likely conducted by script kiddies, who are unskilled cyber threat actors using scripts or automated programs developed by skilled actors. A university website may be defaced for a strategic purpose, but it is more likely that the attack will be opportunistic in nature, conducted by cyber threat actor who found a vulnerability and is seeking to build a reputation. Universities are victimized by web defacements much more often than any other sector. (Figure 4) MS-ISAC monitoring identified nearly 1000 web defacements targeting universities in 2015.

(U) TLP: AMBER Web Defacements Across SLTT Sectors

Figure 4



- *DDOS* attacks are an attempt to make a system unavailable to the intended user(s), such as preventing access to a website. This is accomplished when an attacker successfully consumes all available network or system resources, usually resulting in a slowdown or server crash. The motivation behind DDoS attacks targeting universities can range from financial motivation, for revenge or retaliation, to students

(U) TLP: **AMBER** Case Study: According to open source reporting, in December 2015, a DDoS attack on a network provider for hundreds of universities resulted in the networks of many colleges, universities, and research institutions being unavailable for more than 24 hours.

hoping to get exams pushed back.

- *Scanning and Reconnaissance* is primarily used by cyber threat actors to identify vulnerabilities in programs, servers, or plug-ins that they may exploit, or to determine which attack vector to use in order to gain unauthorized entrance into a system. According to MS-ISAC data, cyber threat actors primarily utilize scanning tools such as Havij, Scanbox, Acunetix, and XT Scan.
- *Hop Points* can occur when the stolen research information or monetary gain is not the end goal for attackers, and instead the system is used as a free host to conduct further malicious activity. Malicious cyber threat actors can use these systems as hop points, masking their real location while potentially establishing that they are from a trusted university IP or email address, which can aid in compromising a more secure target. The non-restrictive research environment prevalent at universities does not always lend itself to secure systems, and as a result, some university systems are likely easier to compromise than other university systems or systems in other sectors.

(U) TLP: **AMBER** Case Study: According to trusted third party reporting, cyber threat actors used a university system (University 1) to host malware and to access and communicate with malware on a system at a second university (University 2). The cyber threat actors used University 1 as a hop point, in order to appear as a credible source to the other university.

(U) TLP: **AMBER** **Content Management Systems:** In 2015, MS-ISAC conducted 4600 notifications regarding potentially vulnerable or out-of-date content management systems (CMS), 200 of which were sent to 41 universities. MS-ISAC is aware of other incidents targeting all but one of the schools that were notified of an out-of-date system, suggesting that cyber threat actors had previously compromised the school in some capacity. This does not necessarily indicate that the path of compromise occurred through the identified CMS, but does show a near 100% correlation between entities running out-of-date systems, and those that become a victim of compromise. MS-ISAC is virtually certain that outdated CMS are the most common attack vector for web system compromises.

(U) TLP: **AMBER** *Each week, the MS-ISAC Vulnerability Management Program (VMP) profiles all the SLTT domains in the database to identify web server software not running the most current version available. The review consists of sending a single request to the home page of a given entity, in much the same way a user on the Internet would browse to the page with a web browser. MS-ISAC then reviews the information for indicators of out-of-date software existing on the system. If out-of-date software is found, the MS-ISAC Security Operations Center sends a notification to the affected entity.*

(U) TLP: **GREEN** **Recommendations:** By employing best practices, universities can best secure systems from malicious cyber threat actors. While such best practices may not prevent malicious activity, they may increase the difficulty cyber threat actors face when attempting to affect the confidentiality, integrity, or accessibility of university networks. General recommendations, such as those below, provide a strong baseline, which should be supplemented by following international and national cybersecurity best practice programs.

- Develop a "realistic" program for patch management that identifies new patches, identifies which systems are vulnerable, downloads the patch from an authoritative source, tests and

verifies the patch in the operating environment, and applies the patch to all devices. MS-ISAC issues Cybersecurity Advisories on critical patches. Anyone may sign up to receive the cyber advisories at http://msisac.cisecurity.org/advisories/.

- Implement intrusion prevention systems (IPS) and/or intrusion detection systems (IDS) and regularly update antivirus software to protect against network intrusions and malware.
- Perform regular vulnerability scans of all systems and address reported vulnerabilities.
- The Center for Internet Security's (CIS) Critical Security Controls for Effective Cyber Defense, Version 6.0, provides a set of specific, prioritized, well-vetted, and supported security actions that organizations can take to assess and improve their current security state. The Critical Controls can be found at: https://www.cisecurity.org/critical-controls.cfm.
- MS-ISAC promotes the Cyber Hygiene Campaign to create nationwide awareness of cyber security issues and make measurable and sustainable improvements. More information on the Cyber Hygiene Campaign can be found at https://www.cisecurity.org/cyber-pledge/.
    1. Count: Know what's connected to and running on your network.
    2. Configure: Implement key security settings to help protect your systems.
    3. Control: Limit and manage those who have administrative privileges.
    4. Patch: Regularly update all apps, software, and operating systems.
    5. Repeat: Repeating each step is essential to maintaining security of your systems.

(U) TLP: WHITE Appendix I contains additional intelligence-driven recommendations for protecting universities against cyber-attacks.

(U) TLP: WHITE *The information in this document is current as of January 1, 2016. Citations are available by contacting the Center for Internet Security (CIS), 31 Tech Valley Drive, East Greenbush, NY 12061, 518-266-3460, IIC@cisecurity.org, www.cisecurity.org.*

(U) TLP: AMBER Source Summary Statement: This report draws on thousands of incidents observed through MS-ISAC sensors, MS-ISAC forensic investigations, and open source reporting, as well as reporting from trusted third parties. All of the reporting is from 2015. MS-ISAC has verified the MS-ISAC and third party reporting and has high confidence in its quality, credibility, and completeness. Where possible the MS-ISAC reporting is derived directly from incident and log analysis, increasing the credibility of the reporting. Open source reporting is verified as possible. However, the reporting is heavily weighted (94%) toward cyber threats to public universities, and not all universities provide reporting to MS-ISAC so there is a possibility of intelligence gaps. Further collection, and reporting from additional universities would reduce these gaps.

(U) TLP: WHITE Appendix I: Best Practice Recommendations

(U) TLP: WHITE *Securing Data Storage and Web Servers*

- PII and PHI should only be stored and transmitted in an encrypted format, according to industry accepted standards.
- Implement logging on web servers, including the Internet Protocol (IP) address of connecting users, user-agent strings, referrers, and host data. Logs should be retained for a minimum of 90 days.
- Implement input validation on web servers to prevent cross-site scripting (XSS) and Structured Query Language injection (SQLi) attacks that may be used in web defacements or data access attempts. SQL More information on SQLi attacks can be found in the MS-ISAC Security Primer on SQLi, available at: https://msisac.cisecurity.org/whitepaper/documents/Security Primer - SQLi.pdf.
- Ensure that your university's Domain Name System (DNS) server and all websites are securely configured.
- Consider implementing a web application firewall or file integrity monitoring system for greater risk management of web applications.
- Ensure network backups include all critical information and test the backups to ensure reinstallation can occur.

(U) TLP: WHITE *Securing Account Credentials*

- Login credentials should be hashed and salted using industry accepted standards. Files storing login credentials should only be readable with super-user privileges.
- Implement frequent password changes and encourage faculty and students to use strong, complex, and unique passwords for all accounts. Passwords should have at least 10 characters and include uppercase and lowercase letters, numerals, and symbols.
- Implement multi-factor authentication consisting of something you know (password) and something you have (mobile phone, physical key, etc.) on social media and online banking accounts, where available.
- Regularly inspect systems for the installation of physical keyloggers.
- Limit user privileges and avoid hosting a remote access single-sign on a network. Using different logins and passwords for each account is recommended.
- Implement login monitoring and generate reports of unauthorized access attempts and access at unusual times or from unusual locations to identify potential intrusions. Logs should be retained for a minimum of one to three months.

(U) TLP: WHITE *Training and Awareness*

- Educate students and staff about the various types of cyber attacks highlighted in this paper, malware, phishing and other types of social engineering attacks.
- Make sure your University IT department is aware of any high profile targets that exist at your university**,** such as CDCs, CAE, or any research departments that fall under the STEM category, which may subject the university to additional targeting.
- Ensure that schools and departments have policy and procedures in place for reporting and reacting to a cyber incident.

(U) TLP: WHITE *DDoS Mitigation*

- Establish and maintain effective partnerships with your Internet Service Provider (ISP) or upstream providers, as they may be able to assist in attack mitigation. If they do not provide DDoS mitigation services, develop the appropriate contacts with a company that does.
- During an attack, provide attacking IP addresses to your ISP in order to implement restrictions at that level, where possible. Apply a firewall filter that restricts traffic to trusted addresses (including the loopback address). Enable firewall logging of accepted and denied traffic in order to determine where the DDoS may originate
- Recommendations for responding to specific types of DDoS attacks can be found in the MS-ISAC Guide to DDoS attacks available at: https://msisac.cisecurity.org/whitepaper/documents/9.pdf

(U) TLP: GREEN Appendix II: MS-ISAC Cyber Threat Actor Definitions

The following definitions below are considered standard by MS-ISAC and are provided to aid in standardizing communications among SLTT governments and Fusion Centers.

(U) TLP: GREEN **Cyber Threat Actor:** A participant *(person, group, or organization)* in an action or process that is characterized by malice or hostile action *(intending or intended to do harm)* towards an environment of computers, information technology, or virtual reality.

- Identified Cyber Threat Actor is an identifiable individual person who participates in malicious cyber activity while explicitly noting they work independent of other CTAs and without claiming allegiance to one cyber threat actor group or movement.
- Identified Cyber Threat Actor Group is an identifiable group of cyber threat actors who claim allegiance to a group or organization that participates in malicious cyber activity.

(U) TLP: GREEN **Profile Types**: CTAs are classified into a variety of groups based on their motivation and affiliation to facilitate discussion and research.

- Nation-State Actors aggressively target and gain persistent access to public and private sector networks to compromise, steal, change, or destroy information. However, not all nation-states have the ability nor pursue sophisticated cyber capabilities and some, while they may have the intent, do not possess the technical competency to achieve such capabilities. Motivation: espionage; Affiliation: nation-states.
- Terrorism Organizations are defined by the U.S. Department of State. Motivation: political or ideological, possibly for financial gain, espionage, or destruction; Affiliation: individuals, organizational, or nation-state.
- Cyber Criminals are largely motivated by profit and represent a long-term, global, and common threat. Cyber criminals may work individually or in groups to achieve their purposes. Motivation: personally financial gain or reputation enhancement; Affiliation: individuals or with co-collaborators.
- Hacktivists, a.k.a. Ideologically-Motivated Criminal Hackers are politically, socially, or ideologically motivated and target victims for publicity or to effect change, which can result in high profile operations. Motivation: political or ideological; Affiliation: individuals or organizational.
- Insiders are a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems. Motivation: generally for financial gain or destruction; Affiliation: current or former employee, contractor, or other business partner who has or had authorized access.