METADATA: THE MOST POTENT WEAPON IN THIS CYBERWAR

THE NEW CYBER-KINETIC-META WAR

JULY 2017

BY JAMES SCOTT
Senior Fellow, Institute for Critical Infrastructure Technology
Metadata: The Most Potent Weapon in This Cyberwar
The New Cyber-Kinetic-Meta War
July 2017

Authored by: James Scott, Sr. Fellow, ICIT
Support ICIT

Information should be liberated, not commoditized.

This powerful philosophy is the bedrock of The Institute for Critical Infrastructure Technology (ICIT), a nonprofit, nonpartisan 501(c)(3) cybersecurity Think Tank located in Washington D.C. Through objective research, publications and educational initiatives, ICIT is cultivating a global cybersecurity renaissance by arming public and private sector leaders with the raw, unfiltered insights needed to defend our critical infrastructures from Advanced Persistent Threats including Cyber Criminals, Nation States, and Cyber Terrorists.

Financial capital from generous individual and corporate donors is the lifeblood of the Institute and a force multiplier to our efforts. With your support, ICIT can continue to empower policy makers, technology executives, and citizens with bleeding-edge research and lift the veil from hyper-evolving adversaries who operate in the dark. Together, we will make quantum leaps in the resiliency of our critical infrastructures, the strength of our National Security and the protection of our personal information.

http://icitech.org/support-icit/
**Contents**

Dragnet Surveillance and Retroactive Legislation Impede Cybersecurity ........................................... 3

Metadata is the New Exploit ......................................................................................................................... 3

S.J. Res. 34 Allows ISPs to Undermine National Security and Privacy ..................................................... 4

Meta-Exploits Are Hyper-Evolving an Already Next Generation Adversarial Landscape ......................... 8
  - Meta-Exploitation Expedites Nation-States Attacks on Critical Infrastructure ................................. 8
  - Meta-Exploitation of Big Data and Metadata Augments Extremist Recruiting .................................. 10
  - Meta-Exploitation of Niche Personnel Enables Cyber-Kinetic Attacks ............................................. 12
  - Meta-Exploitation Unmasks Users with Psychographic and Demographic Algorithms .................. 16
  - Meta-Exploitation Transforms Remote Contractors into Insider Threats ........................................... 17
  - Meta-Exploitation Undermines Democratic Institutions .................................................................. 18
  - Meta-Exploitation Impedes Financial Systems ................................................................................ 19
  - Meta-Exploitation Precisely Tailors Disinformation and Fake News .............................................. 21
  - Meta-Exploitation Disrupts Energy Systems .................................................................................... 22
  - Meta-Exploitation Cripples the Healthcare Sector ........................................................................... 26

Conclusion .................................................................................................................................................. 27

Sources ...................................................................................................................................................... 30
Dragnet Surveillance and Retroactive Legislation Impede Cybersecurity

The combination of dragnet surveillance initiatives and retroactive legislation drastically increase the availability and attainability of exploitable microscopic and macroscopic data pertaining to consumers every online action and decision. Hacking is a resource-intensive grind in which copious exploits work, but few remain functional for long. Naturally, as vulnerabilities are leveraged, or exploits are sold, defenders become aware and develop mitigation and remediation strategies to secure infected networks.

Adversaries are regularly able to find new vulnerabilities to exploit due to the architectonic chaos that plagues the prototypical organizational IoT microcosm. The volume of cyber-attacks continuously increases due to the hyper-evolution of the adversarial landscape and due to the stealth and sophistication of the malicious actors, who become more precise with the direct cyber-kinetic targeting of critical infrastructure executives with elevated privileges. Esoteric and scarce zero-day exploits are no longer essential for the success of a cyber campaign. Instead, adversaries have a new and accelerated focus on the curation of metadata because no matter how much they invest in personnel and training, organizations cannot reduce their reliance on people, and people’s characteristics are difficult or impossible to change.

Metadata enables the success of direct and indirect exploits in all critical infrastructure silos in every major nation because it exposes systemic operational vulnerabilities and it facilitates the bypass of ingrained cyber-hygiene defenses. There are limitless possibilities for social engineering and cyber exploitation when one understands how to make sense of seemingly random metadata or how to pair the data with other exfiltrated data pools in attacks that weaponize psychographic and demographic Big Data algorithms.

Metadata is the New Exploit

Metadata, or “data about data,” is collected and recorded to describe data, identify trends, administer algorithmic solutions, and model potential scenarios. It is categorized as descriptive (identification details), structural (combination and container details) and administrative (creation, technical, and access details). Some metadata, such as that generated from telecommunications, can trivially re-identify parties [1]. That two entities are communicating or have communicated in the past might be valuable information. Other metadata, such as web-browsing info is supposed to be rendered significantly more difficult to use in re-identification methodologies. Social media and online networking sites, applications, and services already associate user profiles, activities, behaviors, and expressions to psychologically manipulate customers to behave in certain ways, absorb specific content, or believe particular details. NSA General Counsel Stewart Baker has been quoted saying, “metadata absolutely tells you everything about somebody’s life. If you have enough metadata, you don’t really need content”
and General Michael Hayden, former director of the NSA and the CIA, adds, “We kill people based on metadata” [1]. If nothing else, metadata enables operators to identify significant sets and associations within greater Big Data stores [2]. Recent legislation, such as mass-surveillance and data sale bills in multiple countries including the United States, has increased the risk that metadata poses to Internet users by allowing or requiring private entities such as ISPs to exchange consumer-centric information with unknown and unregulated third-parties.

Typically, when networks sell data, what they are actually selling is targeting of a particular subsegment of a market on their platform [3]. ISPs cannot do that because they lack a platform to deliver specific ads to specific consumers. Data will have to be conveyed. Further, due to data leakage, insecure ISP servers, and increasing market viability and interest in consumer data sets, it is only a matter of time before Internet users suffer increased adversarial exploitation tailored to their online activities.

**S.J. Res. 34 Allows ISPs to Undermine National Security and Privacy**

S.J. Res. 34 is a 124-word bill (accompanied by a 40-word title) that in its entirety reads, “This joint resolution nullifies the rule submitted by the Federal Communications Commission entitled "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services." The rule published on December 2, 2016: (1) applies the customer privacy requirements of the Communications Act of 1934 to broadband Internet access service and other telecommunications services, (2) requires telecommunications carriers to inform customers about rights to opt in or opt out of the use or the sharing of their confidential information, (3) adopts data security and breach notification requirements, (4) prohibits broadband service offerings that are contingent on surrendering privacy rights, and (5) requires disclosures and affirmative consent when a broadband provider offers customers financial incentives in exchange for the provider's right to use a customer's confidential information.”

Those few sentences undermine consumer privacy and radically redefine the cyber-threat landscape against every critical infrastructure silo. S.J. Res. 34 allows ISPs such as Comcast, Time Warner, Verizon, T-Mobile, etc. to sell consumers’ IP addresses, Internet search histories, temporal data (when a user is online, for how long, the time between clicks, visit duration, etc.), and other metadata. Most importantly S.J. Res. 34 removed requirements that Internet Service Providers: protect data from hackers during storage, transmission, and processing; notify consumers of security incidents that jeopardize their data; and prohibit the unconsented exchange of consumer metadata with private entities [5].

The legislation manifested from ISPs envy of social media and search engine user-data monetization models. Telecommunication companies were barred from participating in these schemes that trade “free” services for customer information for ad revenue because ISPs
capture and process significantly greater quantities and drastically higher detailed information than other online organizations. Their argument that they should enjoy the same liberties and accountability standards as companies like Facebook and Google is intentionally deceptive. Though massive, the aforementioned digital platforms cannot access or capture users’ entire online browsing sessions. They can only monitor user actions on that particular outlet or affiliated sites. Further, social media and search engine companies exchange economic incentives in the form of utility and convenience for users’ data under the express understanding that provided information may be used for targeted advertising or shared with third-parties. Users have some level of choice and consent in what information is provided and how it is used. ISPs offer customers no such additional value. Before restrictions on the sale of consumer data and in the time following S.J. Res. 34, customers will not see a decrease in their Internet and telecommunication bills. If anything, services will continue to increase based on inflated rates that feed profit lines instead of securing consumer data or modernizing decrepit infrastructure. Consumers can choose what information to share on each social media or search engine with which they engage. If the data-price exceeds the user willingness-to-pay, then they seek an alternative or abstain.
Access to the Internet is not comparable. Consumers already pay ISPs exorbitant fees for slow data-exchange-rates and notoriously shoddy customer service. Most do not have any choice in ISP because entire regions lack any alternatives or competition. Meanwhile, telecommunication companies can inspect, monitor, capture, and sell nearly every macroscopic and microscopic datum.

Without S.J. Res. 34, ISPs would have to develop enticing and innovative multi-leveled service platforms to compete with Google, Facebook, and other tech incumbents in the free and fair market. Under S.J. Res. 34, consumers are paying ISPs every month to eventually sell their data to plentiful unknown buyers and resellers to be used for unknown purposes, to be stored on unknown servers with unknown security, and to further transmit to parties unknown. While some nation-state affiliated firms will legally purchase data, most threats cannot and do not
need to do so. Every time a script kiddie, cyber-criminal, or cyber-mercenary infiltrates a public or private sector system, they now have the opportunity to potentially exfiltrate detailed metadata as a secondary objective. Each purchase of metadata sets from an ISP by a legitimate company carries the risk that either that organization’s systems are or will be compromised, that the entity operates in part or whole on behalf of an adversarial nation-state, or that a malicious insider could access and steal the information.

**Figure 2: Comcast is Incapable of Securing Basic Consumer Data**

As shown in Figure 2, Comcast, like Verizon, has failed at securing account data and cannot be trusted to secure and exchange metadata.
Meta-Exploits Are Hyper-Evolving an Already Next Generation Adversarial Landscape

Meta-Exploitation Expedites Nation-States Attacks on Critical Infrastructure

The Chinese state-sponsored Deep Panda APT exfiltrated 22.1 million granular-detailed 127-page SF-86 forms in the 2015 OPM breach. The incident will haunt the U.S. for decades because the entire cleared workforce may already be subject to compromise by the Chinese government. The forms contained the demographic and psychographic information of critical infrastructure personnel and clearance applicants. The stolen information can be aggregated with other data stolen by Deep Panda and affiliated groups, in a custom database of American critical infrastructure personnel. The information was not encrypted in OPM’s system and the only deterrent to establishing a “LinkedIn for espionage and blackmail” is the sheer quantity of data; however, recent advances in Big Data analytics and machine learning will reduce the computational expenditure of leveraging the data [4] [6].

Artificial Intelligence algorithms can combine the data already exfiltrated in the OPM, Anthem, and other incidents with the excessive stores of metadata purchasable from U.S. ISPs. In China, organizations are either owned by the state or are subject to the management of one or more government liaisons who have administrative authority [4]. The Chinese Government can acquire metadata legally through layers of shell companies or foreign branches or by deploying one of around a hundred advanced persistent threat groups to exfiltrate the data from a poorly secured data broker, ISP, or federal agency. In combination with the SF-86 forms, AI can be used to de-anonymize metadata to identify critical infrastructure personnel based on their psychological and web browsing profiles or it can be used to detect vital personnel who have become vulnerable in the years after OPM. Browsing histories that reveal frequent visits to gambling sites, multiple credit card pages, loan applications, or even dating sites, could indicate that a federal employee could be ripe for financial blackmail or transformation into an intelligence asset [6].
Keyloggers from Deep Web are easy to find, download, and use. Figure 3 depicts a minuscule sampling of the thousands of instantly available variants.
Individuals working in niche fields are particularly vulnerable because they can be easily identified in metadata by their visits to sector specific sites and their profiles stand out in the OPM data. Contractors with remote access are particularly appealing targets because their credentials can be infected through spear-phishing, watering-hole, or drive-by-download attacks, and their credentials can be captured with a keylogger. While some might follow protocol and report attempted coercion by a foreign power (likely at risk to their career), others will serve as malicious insiders within secure compounds and vital networks. These individuals can be leveraged to install network backdoors to facilitate future breaches, they can be persuaded to plant logic bombs or wiper malware to cause a cyber-kinetic impact, they could infect sensitive and air-gapped networks with sophisticated malware, or they could personally exfiltrate intellectual property, PII, PHI, state secrets, etc.

**Meta-Exploitation of Big Data and Metadata Augments Extremist Recruiting**

Facebook recently claimed that it implemented a machine learning algorithm that identifies depressed users based on the metadata generated from their searches, clicks, linger time, and other metrics, while on the platform. The intent of the implementation was to alter the content displayed to the user based on their mood, in order to improve the user experience. The company alters the display of content to manipulate the mind and emotions of the user. For all purposes, this is nothing less than privatized cyber-psychological warfare that targets customers, users, and consumers in a campaign that compels them to depend on the product and incrementally increase their daily usage. Essentially, if the user sub-consciously knows that when they use Facebook, their mood improves, then they will rely on it as an emotional crutch [7]. Numerous ad networks and other online outlets have likely developed similar processes for recognizing lonely or troubled consumers as a means of exploiting their melancholy and lapsed judgment to sell goods and services. The same techniques leveraged to detect depressed users could be leveraged by malicious adversaries to locate potential recruits. The only difference is that technology firms and advertising companies are legally allowed to purchase metadata and use it to subjugate the public.

The expansion of ISIL and the Cyber-Caliphate depends on the propagation of extremist media and on the perpetual recruitment of troubled individuals that can be persuaded to act as lone-wolf threat actors. Other far-right and far-left radical organizations similarly operate and depend on active recruitment. Self-polarized lone wolf threat actors are the meta-variant of terrorist. Isolated, depressed, and mentally unstable individuals are prime targets for extremist conscription. These users can be trivially targeted even from pseudo-anonymous metadata because the actual identity of the target does not matter; the threat actor just needs an IP address, email, or social media account to establish initial contact [8].
Lone wolf threat actors turn to the internet for community and purpose. Their online accounts exhibit behaviors of seeking attention, polarization, and further isolation. Many experienced trauma in their youths or are ideologically ostracized in their communities. Before the internet, troubled individuals often did not radicalize to the point of action because in order to do so they had to physically identify, locate, and connect with a tangible local congregation of like-minded individuals. Now on the Internet, radicalization can occur instantly and anonymously within significantly larger and more geographically distributed groups. Statistically, physical membership in hate groups has actually diminished because troubled lone wolves can instantly gratify and cultivate their radical beliefs, they can remotely plan their assaults with online resources (Google Maps, etc.), and they can consume propagandist narratives to model their campaigns around and to assure them that their purpose is worth serving and that their sacrifice will be remembered [8]. Metadata can be leveraged to precisely target attention-seeking and isolated users located in Western nations. Improving the one-to-one recruitment efficiency of extremist networks could provide a second wind to degenerating organizations such as ISIL. Even if recruits are not identified, the metadata could be leveraged to discern emerging trends to inform an optimized evolution of radical propaganda.

The Cyber-Caliphate and similar groups lack the resources and infrastructure of multi-national corporations. They cannot develop powerful algorithms or purchase vast quantities of data. However, they can polarize unsound individuals in foreign nations and use them as malicious insiders within the data broker firms, ISPs, or advertising companies that purchase mass-surveillance Internet information. Moreover, as machine learning and artificial intelligence solutions become more ubiquitous, reliable open source derivatives of efficient algorithms emerge. Additionally, while present in sensitive networks, the lone-wolf could plan attacks, install malware, backdoor systems, or obtain sensitive lists of individual niche personnel to target in their localized assaults.
Metadata may also be used in targeted attacks against high-value critical infrastructure personnel. Location tracking, “super-cookies,” and other technical indicators can be used to physically track a target. Metadata captured by ISPs include Internet usage days and times, duration, and visited top-level domains. Consequently, adversaries can ascertain when someone will be home based on typical usage or determine where they might be based on location tracing or web searches of destinations. Some services, such as Google accounts and mobile applications, even aggregate home and mobile search history and location information within accessible and vulnerable databases. Instead of targeting public spaces, lone-wolves could leverage exfiltrated metadata to target prolific figures or essential critical infrastructure personnel.

Meta-Exploitation of Niche Personnel Enables Cyber-Kinetic Attacks
Critical Infrastructure depends on technical and specialized experts whose knowledge and skill sets often differ from those around them. As a result, metadata could expose the physical or digital locations frequented by niche personnel in the Energy, Financial, or Healthcare sectors. The metadata sold by ISPs after S.J. Res. 34 passed includes top-level domains and may include the IP addresses that frequent those domains. Once a high-profile target had been identified

Smaller ISPs like T-Mobile or AT&T are not better than Comcast and Verizon at protecting consumers’ data.
and profiled using metadata, the adversary can tailor personalized lures. For instance, the attacker could spoof a medical bill, could send them a surgically precise urgent email about a medication for their condition, etc. Alternately, the adversary could release sensitive data to denigrate the individual, to devalue a company through public embarrassment, or to cause any number of personal or societal harms.

Specialized critical infrastructure operators frequent webpages and blogs pertinent to their fields, which are not popular among the uninitiated public. A script kiddie, cybercriminal, techno-mercenary, digital-jihadist, or nation-state sponsored advanced persistent threat (APT), could infect sensitive systems along at least two vectors. An attacker could focus on a specific IP address connected to a target operator. Cyber-attackers could use metadata to determine the most popular niche sites. Energy, healthcare, or financial sector organizations’ webpages or online portals might qualify as niche sites. Next, they could compromise those sites using script kiddie tools that are freely available on Deep Web markets and forums, or they could infect an employee system via social engineering (site admins and contributors can be identified in metadata as the most frequent and prolonged visitors) and then laterally compromise the page. The compromised site can then be used as a “watering-hole” to evaluate visiting system parameters and to deliver customized malicious payloads. In this manner, a single attacker leveraging only a small pool of localized metadata might compromise every niche expert in a region [6].
The adversary could launch a multi-vector precision targeted spear-phishing and social engineering campaign that bombards the victim with spoofed emails carrying malicious payloads, from expected sources. One example would be a spoofed newsletter from a niche site. Each hyperlink might redirect the target to a drive-by-download landing page for a fraction of a second. In that brief time, their system could be infected with a single or multi-stage malware dropper. The dropper could deliver any number of malware to the victim system provided it uses obfuscation mechanisms (such as a mutagenic hash) sufficient to bypass consumer anti-malware applications. Another spear-phishing email might contain a malicious attachment that delivers malware by exploiting a zero-day or disclosed vulnerability in the Microsoft application suite.

Figure 5: Tools to Create Watering-hole and Drive-by-Download Links are Cheap

Metadata can tell attackers what sites are visited by niche personnel, C-level executives, entry-level staff, voters, or any other demographic. Script kiddie tools can be used to generate malicious landing pages and drive-by-download links. Metadata can also be paired with psychographic and demographic Big Data algorithms to create tantalizing fake news pages.
The fake newsletter might also appear to refresh the page and land the user on a spoofed login page for their email client. The adversary captures any credentials entered into the page before it redirects the unaware user back to their inbox. Since far too many un-cyber-hygienic users reuse the same or slightly altered credentials across a broad range of sites or link their diverse accounts to a single email address, the captured credentials might grant the actor access to all facets of the target’s life. At a bare minimum, the adversary can send malicious emails from the legitimate account to trusted contacts that may operate within the same or similar organizations.

Stuxnet demonstrated that infections spread from foreign media could hobble an Energy operation. Most organizations now operate under a BYOD policy. Systems infected via the aforementioned watering-hole, drive-by-download, or spear-phishing attacks may bring malware into the network or across an air-gap. BlackEnergy demonstrated the viability and devastation of such an attack. On December 23, 2015, BlackEnergy infected the Prykarpattyaoblenegro power plant in Ukraine and caused a severe outage. More significant than the immediate loss of power, the threat actor, who is likely backed by the Russian state, demonstrated that the malware, which has been regularly discovered on U.S. networks, can severely cripple a nation’s critical infrastructure as part of a cyber-physical campaign. The potency of BlackEnergy derives from its wiper component, which can erase or brick systems upon which vital operations depend. Wipers are increasingly becoming more prevalent and easier to spread. Early analysis of the “NotPetya” malware spread to over 2000 systems on June 27, 2017, appears to have been a wiper malware disguised as ransomware. The self-propagating malware spread via the EternalBlue exploit that leverages the MS17-010 SMB vulnerability on unpatched Windows systems. Unlike the WannaCry ransomware attack before it, “NotPetya” was designed to not spread outside target networks and it did not include a kill-switch. Consequently, the attack may have been a trial run of a widespread wiper attack. Oil infrastructure and the Chernobyl facility were infected, but the impact was limited. WannaCry spread through unpatched legacy technology and infected diverse sectors ranging from Energy to Healthcare to Government. The “NotPetya” malware may have been spread via spear-phishing or a poisoned accounting software update, but it still impacted Energy, Transportation, Legal, and other sectors [9]. Future wiper campaigns that rely on exfiltrated metadata could precisely target only the Energy or Healthcare sectors in specific regions or states, by first infecting systems belonging to the niche personnel whose devices connect to those sensitive networks.
Meta-Exploitation Unmasks Users with Psychographic and Demographic Algorithms

Psychographic and demographic Big Data analytics can be used to re-identify individuals based on metadata about that person. For instance, everyone has a medical profile that is created from medical metadata. In 1997, Massachusetts Governor William Weld was re-identified within regional pseudo-anonymized medical data by pairing the set with a voter registry [6].

Similarly, every user has a distinct web traffic profile. They visit particular sites, use the Internet at certain times, and browse pages in discernable patterns. Internet users are slaves to their rhythmic subconscious behaviors. How many users start their workday by logging on, checking email, and then navigating to the same two or three news sites or web portals? Cybercriminals can capitalize on psychographic and demographic re-identification in lucrative blackmail schemes against any politician or public figure that can be linked to unconventional or embarrassing online activity. A more sophisticated adversary, such as a state-sponsored advanced persistent threat might compel the victim to exfiltrate information or act according to certain instructions. Domestic and Foreign Intelligence and Counter-Intelligence assets may also be re-identified, profiled, and compromised through the increasingly widespread availability of metadata.

Very few, if any, Internet users are proud of all of their online activities. The adversarial application of psychographic and demographic Big Data analytics can potentially undermine democracy and jeopardize national security [6]. Re-identification could also be used to “catfish” or lure victims on gaming, dating, or social media sites into relationships under the misapprehension of romance, friendship, etc. Afterward, the attacker can elicit the exchange of more incriminating communications. The mistakenly trusted adversary might be able to deliver a malicious payload via email, social media, or another medium, that the victim normally would not click on or download. In the past, the Duke-family of APT demonstrated that even videos and images could be potent malicious attachments [10]. Typical payloads would include tools that capture the victim’s screen, establish a persistent presence on the system, covertly activate the microphone and/or camera and record audio or video, log keystrokes, exfiltrate files, and allow for the remote execution of code on the system. After the adversary has exhausted the utility of the victim, they might leverage stolen credentials to access sensitive systems or send additional social engineering lures through compromised accounts. The threat of embarrassment or public shame alone could be enough to coerce a victim to act as an insider threat.
Meta-Exploitation Transforms Remote Contractors into Insider Threats

State Election Commissions are under-resourced, under-staffed, and over-burdened with antiquated proprietary black-box election systems that have not been phased out despite inherent security vulnerabilities. Many states manage their election systems through a combination of paid officials, volunteers, and election manufacturer employees. Some states also rely on external “Election Consultants” to remotely update and manage Voting applications and systems. The consultant has remote access and unrestricted control of managed systems. Reports suggest that in the past, consultants have even uploaded their own versions of election software to systems without the knowledge or consent of election officials. A single consultant might manage the elections for multiple counties or states from a remote location [11].

Election managers are already tenuous and potential security liabilities. Bidding contractors tend to falsify information, and holistic background checks are rarely conducted on them. Some
work independently from their home, with no legal regulations on the security of their devices. Election consultant organizations regularly rebrand to attract new clientele.

These consultants act as “first responders” to any suspicious activity detected on election applications and networks. Because they are hired when the Election Commission lacks the prerequisite technical expertise, they essentially police their own activity on systems. If the PC or laptop used to remotely access and manage election systems is infected with malware, that code could be laterally transmitted to the central tabulator or another subcomponent [11]. Using metadata collected from dragnet surveillance or ISPs, an adversary can easily identify and target a remote Election consultant. After all, web-portals connecting to election systems are uncommon online destinations, and connecting traffic from outside the region or state can easily be traced back to its source. Adversaries may target the individual with social engineering, spear-phishing, watering-hole, drive-by-download, or Man-in-the-Middle attacks. Malicious droppers, RATs, keyloggers, or credential stealers may be planted on their systems. Malware might be directly delivered to election systems, or the threat actor might auction Access-as-a-Service.

Meta-Exploitation Undermines Democratic Institutions
Despite irrefutable proof of the vulnerabilities inherent in outdated black-box proprietary voting systems, local and state election officials insist that malicious campaigns would be extremely difficult or impossible due to stringent security and access requirements. They fail to recognize that many machines remain remotely vulnerable to infection through poisoned updates, attacks on the central tabulator, or other modern vectors, which the nearly two-decade-old systems were not designed to repel [11]. Officials themselves are proportionally identifiable and exploitable in relation to the prevalence of metadata because few users connect to specialized election official web-portals. Recent reports allege that a malicious adversary compromised a voting software vendor’s systems and sent 122 spear-phishing emails infected with malware to election officials. The registration and voting systems of 39 states may have been compromised in 2016 as a result. While there is no evidence of an influence on the outcome of the 2016 election, by spreading infected election management software, an attacker could infect individual ballot machines or central tabulators on Election Day. Officials argue that the decentralization of voting systems and processes sufficiently secures them against adversarial compromise; however, if a threat actor infects the central tabulator or poisons a widely-distributed application or update, then the entire process is invalid [12]. Metadata and historical voting records can be used to predict the voting record of a region within a margin of error. To alter the outcome of an election without arousing suspicion or inciting a full recount, attackers only need to ensure that the altered outcome lies within the allotted error. Full recounts consume time and resources and are rarely conducted [11]. Further, for some states, the candidate challenging the result must pay for the audit.
Grassroots and even mainstream candidates tend not to be able to afford the price of an audit immediately after a contentious election and within the time-frame specified for audit requests.

**Meta-Exploitation Impedes Financial Systems**

Research into businesses, periodic consultation of stock prices, and secure connections to financial institutions can reveal financial sector personnel within Metadata sets, to cybercriminals, digital mercenaries, and nation-state APTs. Threat actors need only identify financial personnel and deliver novel variants of Deep Web malware to reap immense fiscal gains. Consider the estimated $1 billion success of the Carbanak APT [13].

The Carbanak group is a criminal advanced persistent threat group whose attacks against at least 100 financial organizations at 300 IP addresses located in approximately 30 countries including Russia, the United States, Germany, China, and Ukraine, resulted in an estimated $1 billion in losses in the first half of 2014. The group relied on a spear-phishing campaign that delivered sophisticated malware that was developed from code widely-available on Deep Web markets and forums. Analyzed malicious attachments reveal that the attackers exploited vulnerabilities in Microsoft Word 2003, 2007, and 2010 (CVE-2012-0158, and CVE-2014-1761).

After successful exploitation of a vulnerability, the shellcode decrypted and installed the Carbanak backdoor on the victim host. The Carbanak backdoor installed and then it re-installed a renamed copy of itself into “%system32%\com” as “svhost.exe” with system, hidden, and read-only attributes. After installation, the backdoor connects to its C2 server through HTTP (with RC2+Base64 encryption) and downloads a file (kldconfig.plug) which details which process to monitor. The kit sets the Termservice service execution mode to auto in order to enable Remote Desktop Protocol (RDP). The backdoor provided access to the intranet of the victim organization. Next, the adversary probed the intranet for other vulnerable targets and specifically for critical financial systems. Typically, tens to hundreds of computers were infected before an admin system, with the necessary access, was compromised. If banking applications such as BLIZKO or IFOBS are discovered, then a special notification is sent to the C2 server to notify the adversary that financial systems were discovered. Keyloggers, screen capture, and remote monitoring tools were deployed on infected financial systems. The actors wanted to learn as much as possible about the digital environment, relevant applications, and institutional processes prior to initiating financial transfers via a remote administration tool (that was whitelisted and installed by the system administrators of the corporate environment). The learned proficiency within the system and the compromised credentials and cryptographic keys precluded the need for additional exploits [13].

Obviously, not every cyber-criminal will have the sophistication, resources, or patience of an APT such as Carbanak; however, following the initial deployment of a backdoor or RAT on the
financial system identified through metadata, a threat actor could sell Access-as-a-Service, deploy ransomware, spread a botnet, or financially capitalize on the compromise through any number of alternative vectors that result in immediate fiscal gains for minimal resource expenditure.

**Figure 7: Exploit Kits are Adaptable to the Victim**

RATs and other tools can easily be tailored to the victim. Metadata can guide hackers in preplanning that customization.

Financial C-level management, who already face significant public and professional scrutiny, may be particularly susceptible to re-identification and compromise. The access permitted to their credentials may exceed what is necessary for their duties. Information Security personnel may hesitate to question activity associated with C-level accounts. Further, the reputational and organizational impact resulting from the internal compromise, loss of millions or billions in funds, and public outcry, will be more significant if a C-level executive is found responsible.
Meta-Exploitation Precisely Tailors Disinformation and Fake News

The exchange of granular consumer metadata increases the potential impact, pervasiveness, and ubiquity of fake news, propagated false narratives, and propaganda. This vector is not new, but it has recently increased in popularity. Russia’s “the Agency” spread diverting opinions and consternation for years [14]. North Korea has a similar bureau. Cyber adversaries tailor spear-phishing emails and craft malvertising lures to capitalize on cyber-hygieneically inept users’ need to follow links and view attachments. Lures range in complexity from precise, error-free custom tailored spear-phishing emails that leverage the target's LinkedIn profile, to typo-riddled inflammatory spam articles; however, the focus of every social engineering campaign is to entice a target demographic of users to share information, to open an email, to download an attachment, to visit a watering-hole site, etc. For cyber adversaries, social engineering campaigns are low risk, high probability of success, low investment, and high reward. The first victim covers the resource cost of the campaign, and each additional victim is a positive gain.

News, fake news, propaganda, and disinformation campaigns are multi-vector attacks designed to infect victim systems and to spread competing false narratives, disinformation, and discord. The resulting conflict of “facts” and clashing of opinions undermines democracy and weakens national security [10].

Individuals feel compelled to pay attention to prolific headlines, trending stories, and major outlets; especially when the subjects are sordid, tragic, alarming, or topical. Their trust for legitimate and known news organizations assuages any caution when following a link or opening an attachment. Adversaries may compromise legitimate popular news sites and utilize them as watering-hole sites or purchase banner space on the sites and redirect visitors to malicious landing pages. Search history information and top-level domain content made available through the sale and insecure storage, transmission, and handling of highly sensitive metadata enables adversaries to optimize their disinformation campaigns for regions, for specific targets or targets in a specific sector [10].

Recently, fake news articles have emerged as a new social engineering vector that leverages psychological attributes and interests of targets against their ingrained cyber-hygiene training and awareness. Victims interact with news lures for a number of reasons, which include a drive to be “up-to-date” or current; a sense of urgency; socio-political polarization; curiosity; or fear. The most effective lures either incorporate a real news article as an attachment, as a malicious link to a compromised site, or as a tantalizing banner bordering an article tailored to the potential victims. For instance, in 2014, the Sochi Olympics, the World Cup, the death of Robin Williams, the leak of celebrities’ private photos from the iCloud, global disasters, and other stories were used as lures by advanced persistent threat groups such as the Chinese state-sponsored Naikon APT, which has launched spear-phishing campaigns into organizations surrounding the South China Sea since 2010. It targets geo-political intelligence from civilian
and military government organizations in the Philippines, Malaysia, Cambodia, Indonesia, Vietnam, Myanmar, Singapore, Nepal, Thailand, Laos, and China [10]. Russian APTs such as PinchDuke, CosmicDuke, APT 28, APT29 and Hammertoss, have used real or fake news lures in past campaigns. Cybercriminal APTs like Dropping Elephant and cyber-terrorist APTs like the Moonlight APT have also incorporated news lures into their campaigns.

In 2016 and 2017, APTs and cybercriminals, popularized malicious political fake news lures. During the 2016 election cycle, election systems, including voter registration records, were targeted in 39 states, DNC systems were compromised, and data analytics subcontractors exposed over 200 million RNC registration records in plaintext without security controls [12] [15]. When tailoring a fake news or any other attack, the prevalence of more personal information is directly proportional to the probability that the target will respond to the lure. Combining exposed voter registration records with purchased or exfiltrated metadata empowers threat actors to craft tantalizing or infuriating political and issue based lures that bypass victims’ cyber-hygiene training and awareness to spread malware, competing false narratives or polarizing information amongst typical voters and between extreme left-wing and right-wing communities.

**Meta-Exploitation Disrupts Energy Systems**

Whale-phishing is the practice of precision targeting a privileged or lucrative victim within a subset of potential targets. The metadata erroneously and insecurely stored within private and public sector databases and naively sold by ISPs facilitates attacks on system administrators and corporate executives. Metadata exacerbates the cybersecurity vulnerabilities and liabilities lingering from the transition into the digital age. Training the C-suite to understand, care, and practice cybersecurity and cyber-hygiene are already one of the greatest challenges of Information Security professionals. No one wants to dictate instructions to their bosses. Information Security personnel in hierarchical sectors are already struggling to combat the tendency of superiors deciding they are personally exempt from security policy and best practices.

The U.S. Energy sector consists of 7,000 power plants, 55,000 substations, 160,000 miles of high-voltage transmission lines, and 66 balancing authorities. Modernization is complicated by the size of the grid and the necessity for the constant transmission of power [16]. Targeting the C-suite may be an attacker’s best chance of spreading a persistent and sophisticated malware onto the network because management often (unnecessarily) has administrative credentials that exceed the needs and duties of their role within the organization and because most personnel will follow lures sent from their superiors.

The sector is targeted by Russian APTs like Energetic Bear, Uroburos, Sandworm, CosmicDuke, MiniDuke, and numerous others. Chinese APTs, Axiom, NetTraveler, Deep Panda, etc. also
attack Energy systems. Chinese APT 3 even launches whale-phishing campaigns against Energy executives. Iranian Tarh Andishan, cyber-mercenary Dropping Elephant, cyber-terrorist collectives such as the Cyber Caliphate, and hail-mary threat actors focus their attacks on the sector because it relies on legacy systems, because every citizen is a customer to the sector, and because attacks against the grid have the greatest potential for cyber-kinetic impacts. Altering electricity distribution parameters, redirecting pipes, pressure, or flow, or any number of minuscule deviations from operational norms can result in disproportionately impactful cyber-kinetic results such as blackouts, burst pipelines, etc. Many within the Energy sector still rely on security-via-obscurity or decentralization-as-security instead of modernizing to layered defense-grade solutions that incorporate artificial intelligence and machine learning.

Figure 8: Mercenary Hackers are Available

Mercenary hackers are cheap, accessible, and common on Deep Web markets and forums. Their services are frequented by script kiddies, cyber criminals, hail-mary threats, cyber-jihadists, and other attackers in multi-layered campaigns.
Compromising a naïve or “old-world” executive is an attacker’s greatest opportunity of severely compromising or crippling an Energy organization. The negligent exchange of metadata exposes personal preferences, interests, and communications of Energy executives. Every variety of adversary can leverage that information in precision tailored social engineering or watering-hole attacks. Those without the technical means, such as hail-mary threats, may outsource the initial infection or stages of the multi-vector attack campaign to cyber-mercenaries. For instance, a hail-mary actor like North Korea might hire one or more cyber-mercenaries to disrupt an Energy organization. After using Metadata to profile, target, and whale-phish an Energy C-level, or using metadata to identify and compromise a less secure site where they reuse credentials, a cyber-mercenary might send additional phishing emails to lower level personnel or sell access-as-a-service to additional attackers. The hail-mary actor might disrupt distribution, interfere with the parameters of legacy systems, deliver wiper malware, or launch a cyber-kinetic attack on the grid.
Even adversaries who lack technical skills enough to exploit metadata can use it to launch tailored attacks by contracting cyber-mercenaries on Deep Web forums. Script kiddies, cyber-jihadists, hail-mary threat actors, and APTs outsource layers of their attacks. The market is so fruitful that many operations have begun recruiting additional talent. The practice has become so normalized that the listings resemble traditional job postings.
Meta-Exploitation Cripples the Healthcare Sector

Figure 10: The Healthcare Sector is Plagued by Custom Ransomware and Ransomware-as-a-Service

The healthcare sector guards a treasure trove of valuable and highly sensitive electronic healthcare records. As a resourceful yet significantly vulnerable economic category, it is also the frequent victim of ransomware campaigns. For instance, the May 12, 2017, WannaCry attack infected 48 NHS Trust facilities in the UK. One of the challenges of securing medical systems is that healthcare facilities rely on numerous staff from diverse backgrounds and on patient security [17]. If a single infected BYOD device enters a hospital, the medical network connecting multiple hospitals could be infected and crippled in minutes or hours. Recent efforts have attempted to modernize medical systems, protect medical devices behind layered security, and train staff in basic cyber-hygiene. The forfeiture of metadata detracts from that progress by...

The healthcare sector is submerged in a ransomware epidemic. Healthcare systems are particularly susceptible to ransomware because they are antiquated and because lives are jeopardized every minute that they are offline. Ransomware-as-a-Service and customized malware can be purchased from Deep Web stores such as the Rainmaker Labs pictured in Figure 10. The adoption of modernized systems and layered defenses will do little to deter the onslaught of malicious campaigns if adversaries can precision target exhausted, over-exerted, and un-cyber-hygienic personnel in metadata-driven social engineering campaigns.

The healthcare sector guards a treasure trove of valuable and highly sensitive electronic healthcare records. As a resourceful yet significantly vulnerable economic category, it is also the frequent victim of ransomware campaigns. For instance, the May 12, 2017, WannaCry attack infected 48 NHS Trust facilities in the UK. One of the challenges of securing medical systems is that healthcare facilities rely on numerous staff from diverse backgrounds and on patient security [17]. If a single infected BYOD device enters a hospital, the medical network connecting multiple hospitals could be infected and crippled in minutes or hours. Recent efforts have attempted to modernize medical systems, protect medical devices behind layered security, and train staff in basic cyber-hygiene. The forfeiture of metadata detracts from that progress by...
directing attackers to which sites to infect as watering-holes, where to place drive-by-download banner ads, or even which devices to infect. Chances are that the next stop for visitors to WebMD or similar digital diagnoses services is a medical facility. Similarly, the PHI networks, cloud services, niche journals, and telecommunication channels employed by medical professionals can likely be used to identify them. Doctors, nurses, administrators, and other medical staff are notoriously stressed and distracted. They are prime targets for adversarial exploitation. Further, many resort to unsavory vices to mitigate the pressures of their work. Enterprising adversaries could leverage their distraction with “urgent” spear-phishing emails to infect medical networks with ransomware, cyber-kinetic malware, or other malicious code, or they could blackmail medical professionals with their online metadata to entice them to exfiltrate IP, PII, or EHR, or to infect network systems. Once the system is infected with a persistent backdoor, the adversary can sell Access-as-a-Service, or they can spread ransomware, RATs, keyloggers, password dumpers, or other malware that captures the screen, camera, or microphone, onto critical systems. The adversary can exfiltrate and sell PII and EHRs on Deep Web markets and forums. The combination of these records and metadata may increase the utility and value of “Fullz.” In addition to identity theft, blackmail, financial fraud, etc. adversaries will find novel vectors to further exploit patients based on their medical information and metadata. The potential cascading impacts are unparalleled because hackers will own both "who a victim is" and "how a victim behaves." Patients, who may not be aware of the compromise, cannot change the fundamental and biological characteristics of their identity. Consequently, attackers will virtually own the victim for years or decades. It is a close wager whether malicious hackers, negligent ISPs, or irresponsible healthcare organizations will capitalize most on the fate of patients' whose essential identity was packaged as metadata and sold to any entity with a budget.

**Conclusion**

Metadata is collected and sold by negligent and avaricious ISPs at a severe risk to consumers, private businesses, federal entities, and national security. Energy, Healthcare, Finance, Defense, and every other sector are violently susceptible to the precision targeting of C-level executives, niche personnel, average consumers, etc. facilitated by the adversarial adoption and malicious exploitation of users microscopically detailed Internet browsing histories and behaviors used in combination with existing social engineering schemes, exploit kits, and sophisticated custom malware. When paired with Big Data psychographic and demographic algorithms, artificial intelligence, and machine learning, metadata catalyzes and optimizes fake news, propaganda, disinformation, and false narrative campaigns which undermine democratic institutions, national stability, and economic markets. Cyberwarfare is already being waged in the kinetic, digital, and mental realms using metadata as the primary weapon to successfully target and compromise public and private entities. Regulating the exchange of customer information,
limiting dragnet surveillance initiatives, mandating the security of data in transit, storage, and processing and prohibiting ISPs from haphazardly and negligently capitalizing from their paying customers, are the only ways to mitigate the emerging meta-data driven cyberwar.
ICIT Contact Information

Phone: 202-600-7250 Ext 101

E-mail: http://icitech.org/contactus/

ICIT Websites & Social Media

www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

https://www.facebook.com/ICITorg
Sources


