ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

How to Crush the Health Sector's Ransomware Pandemic

The Machine Learning Based Artificial Intelligence Revolution Starts Now!

March 2017

Authored by:

James Scott (Senior Fellow, Institute for Critical Infrastructure Technology)

Contents

Introduction 4

Health Sector 6

Machine Learning in Healthcare Cybersecurity 13

Ransomware 16

The Future of Algorithmic Defenses 23

Barriers to Adoption 25

Conclusion 26

Sources 28

How to Crush the Health Sector's Ransomware Pandemic:

The Machine Learning Based Artificial Intelligence Revolution Starts Now

March 2017

Authored by: James Scott, Sr. Fellow, ICIT

Thought Leader Contributions from the Following Experts:

- **Rob Bathurst, ICIT Fellow and Worldwide Managing Director, Cylance**
- **David McNeely, ICIT Fellow & VP Product Strategy, Centrify**
- **Robert Lord, ICIT Fellow & CEO, Protenus**
- **Rick Caccia, ICIT Fellow & V.P., Exabeam**
- **Don McLean, ICIT Fellow & Chief Technologist, DLT**

Upcoming Events

The 2017 Critical Infrastructure Forum

June 7, 2017, The Four Seasons Washington D.C.
www.icitforum.org

The 2017
Critical Infrastructure Forum
Rise of The Machines
June 7, 2017
The Four Seasons - Washington D.C.

ICIT Briefing - Artificial Intelligence & Machine Learning – Leading Cybersecurity’s Paradigm Shift

March 28, 2017, The National Press Club Washington D.C.
http://icitech.org/event/icit-monthly-briefing/

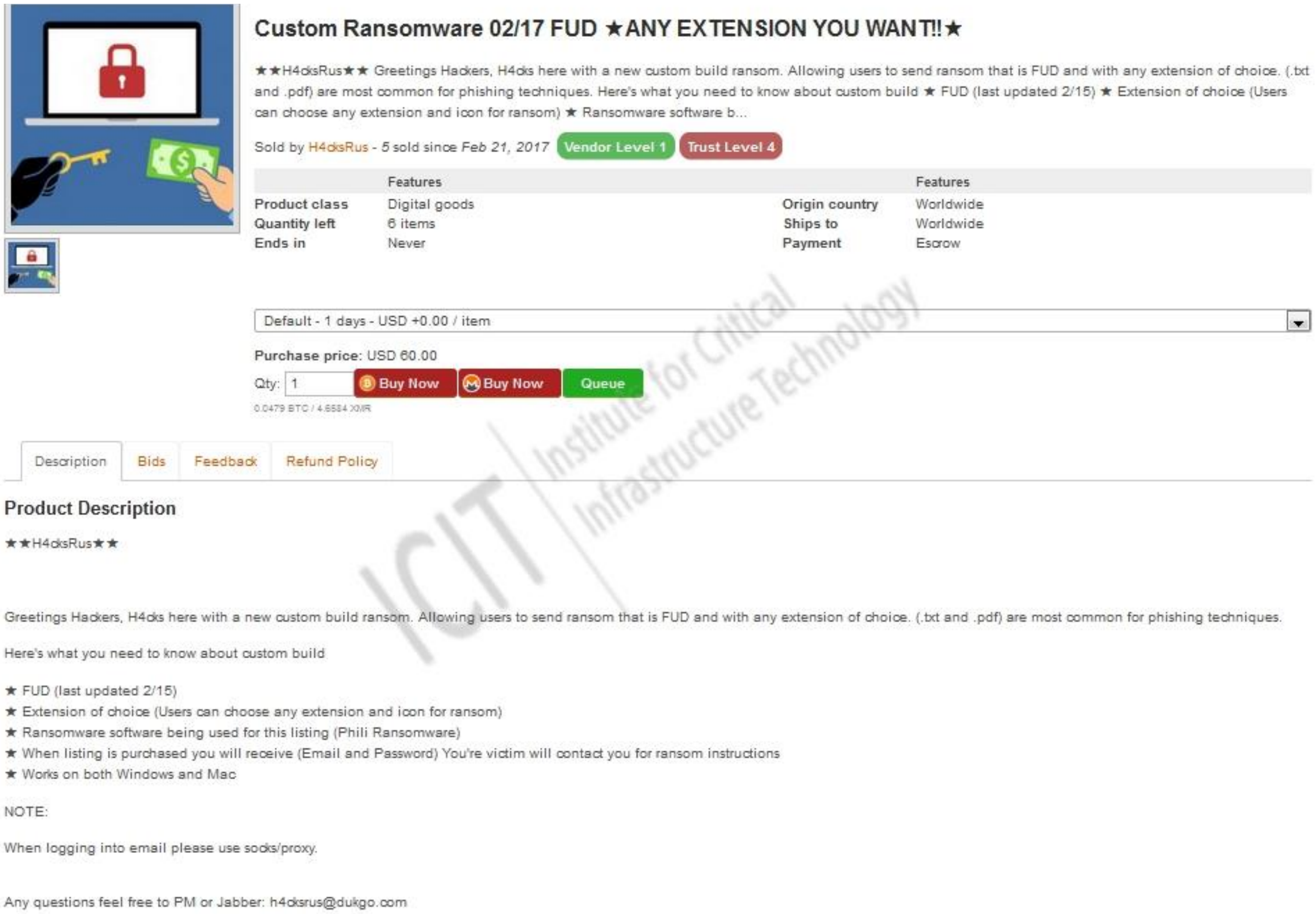
Visit the ICIT Library to view additional research and publications
https://www.amazon.com/James-Scott/e/B01IPLQKSQ/ref=dp_byline_cont_pop_ebooks_1

Introduction

Signature based malware and ransomware detection is dead. In an age of dynamic malware obfuscation through operations such as mutating hash, a hyper-evolving threat landscape, and technologically next generation adversaries, offensive campaigns have an overwhelming advantage over defensive strategies. Adversaries are simply too numerous and too adaptive for security professionals to predict and preempt. Further, the threat landscape is decidedly asymmetric. Organizations spend immense budgets to hire seasoned information security experts, to implement the latest security solutions, and to protect their data according to public good and the increasing tide of regulations and standards; only to be comically overcome by numerous adversaries who invest relatively minuscule resources other than time and dedication.

A single spear-phishing email carrying a slightly altered malware can bypass multi-million dollar enterprise security solutions if an adversary deceives a cyber-hygienically apathetic employee into opening the attachment or clicking a malicious link and thereby compromising the entire network. Solutions to mitigate this attack vector are ineffective and cost anywhere from thousands to hundreds of thousands of dollars. Training personnel to eschew the lures has likewise proven fruitless, especially in fields such as healthcare, where priorities such as saving the most lives in the least time, supersedes concerns of cybersecurity. Meanwhile, sending hundreds or thousands of malicious social engineering lures costs adversaries pennies. After all, they need only one employee in one of the target organizations to respond to the lure in order for their campaign to succeed. But what if an organization could inject machine learning based artificial intelligence throughout the layers of their IoT microcosm? What if there was a way to not only detect and respond to threat, but also predict by way of virtually, omnipresent, algorithmic defense?

Figure 1: Custom Fully Undetectable (FUD) Ransomware on Alphabay Deep Web Market



Custom Ransomware 02/17 FUD ★ANY EXTENSION YOU WANT!!★

★★H4cksRus★★ Greetings Hackers, H4cks here with a new custom build ransom. Allowing users to send ransom that is FUD and with any extension of choice. (.txt and .pdf) are most common for phishing techniques. Here's what you need to know about custom build ★ FUD (last updated 2/15) ★ Extension of choice (Users can choose any extension and icon for ransom) ★ Ransomware software b...

Sold by H4cksRus - 5 sold since *Feb 21, 2017*

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	6 items	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 60.00

Qty: 1

0.0479 BTC / 4.6584 XMR

Product Description

★★H4cksRus★★

Greetings Hackers, H4cks here with a new custom build ransom. Allowing users to send ransom that is FUD and with any extension of choice. (.txt and .pdf) are most common for phishing techniques.

Here's what you need to know about custom build

★ FUD (last updated 2/15)
★ Extension of choice (Users can choose any extension and icon for ransom)
★ Ransomware software being used for this listing (Phili Ransomware)
★ When listing is purchased you will receive (Email and Password) You're victim will contact you for ransom instructions
★ Works on both Windows and Mac

NOTE:

When logging into email please use socks/proxy.

Any questions feel free to PM or Jabber: h4cksrus@dukgo.com

Figure 1 depicts a custom ransomware that is listed on the Alphabay Deep Web as fully undetectable by traditional anti-virus and legacy technologies.

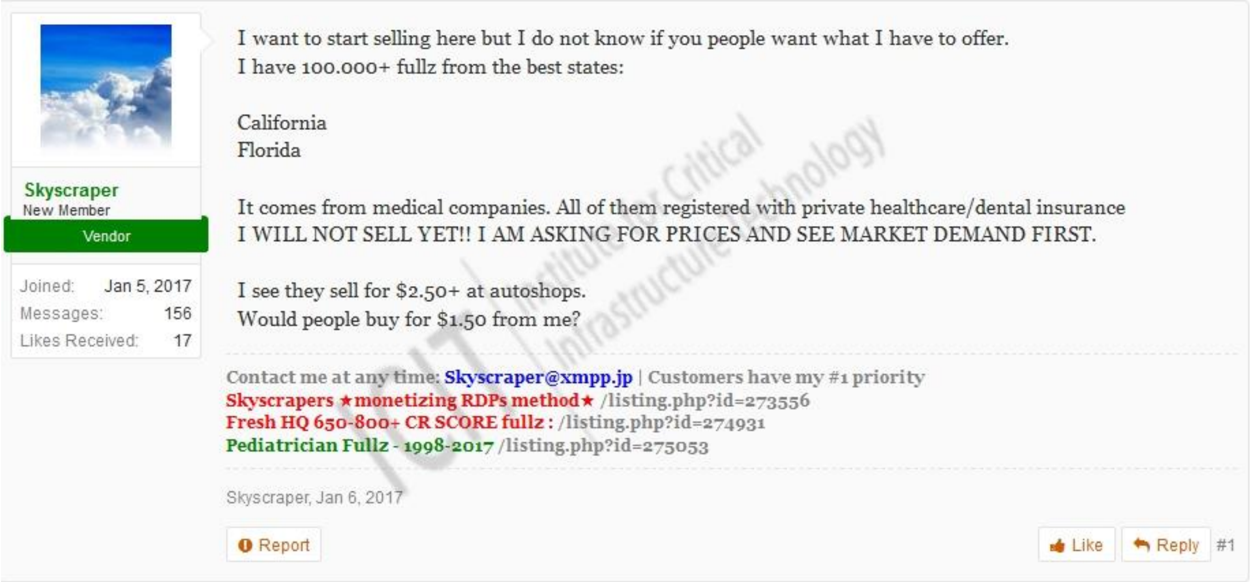
Few critical infrastructures need to expedite their cyber resiliency as desperately as the health sector, who repeatedly demonstrates lackadaisical cyber hygiene, finagled and Frankensteined networks, virtually unanimous absence of security operations teams and good ol' boys club bureaucratic board members flexing little more than smoke and mirror, cyber security theatrics as their organizational defense. The health sector will continue to be pummeled by any and every script kiddie and sophisticated cybercriminal dedicated to exfiltrating electronic health records and PII for infinite variation of use and optimal capitalization on dark web forums.

In this cyberwar, industry is on their own and must combat nation states, cyber mercenaries, cyber caliphate and other actors via layered security laced with intelligent machines.

Health Sector

In 2016, the health sector was pummeled by ransomware attacks, insider threats, APT campaigns, and other cyber-attacks designed to distract, consume resources, profit by compromising the confidentiality, availability, or integrity of critical health systems, or to outright exfiltrate sensitive EHR, PII, IP, and other data [1]. The healthcare industry is the primary perpetual target of cyber attackers due to the massive amounts of disparate data collected, stored, and inadequately protected. Early adoption of sophisticated algorithmic defenses such as machine learning or artificial intelligence solutions will transform healthcare cyber defenses beyond the capabilities of average attackers [2]. Exabeam's Rick Caccia, an ICIT Fellow, describes, "Artificial Intelligence and Machine Learning bring the same value to healthcare security that they bring to other industries: using big data analytics to detect threats and assist in response. Machine Learning [ML] can be applied to two useful areas in healthcare cybersecurity. The first is using ML to link seemingly unrelated activities together. For example, a hacker might use multiple accounts to access different types of sensitive PHI info. Each account might have valid access rights to some of the data, so rules-based security solutions won't see anything wrong. ML can track IP address and other identifying information to link the parts into a single unified session that is then positively attributed to a person. The second is to then assess the behaviors of those coherent identities to determine if risky behavior is underway." The healthcare sector is already utilizing cognitive and AI solutions for big data analytics and for clinical applications. Now, the industry needs to responsibly protect its patients and their data by adopting algorithmic defense solutions.

Figure 2: Healthcare Data Exchange on Deep Web Forums



Skyscraper
New Member
Vendor

Joined: Jan 5, 2017
Messages: 156
Likes Received: 17

I want to start selling here but I do not know if you people want what I have to offer.
I have 100.000+ fullz from the best states:

California
Florida

It comes from medical companies. All of them registered with private healthcare/dental insurance
I WILL NOT SELL YET!! I AM ASKING FOR PRICES AND SEE MARKET DEMAND FIRST.

I see they sell for $2.50+ at autoshops.
Would people buy for $1.50 from me?

Contact me at any time: Skyscraper@xmpp.jp | Customers have my #1 priority
Skyscrapers ★monetizing RDPs method★ /listing.php?id=273556
Fresh HQ 650-800+ CR SCORE fullz : /listing.php?id=274931
Pediatrician Fullz - 1998-2017 /listing.php?id=275053

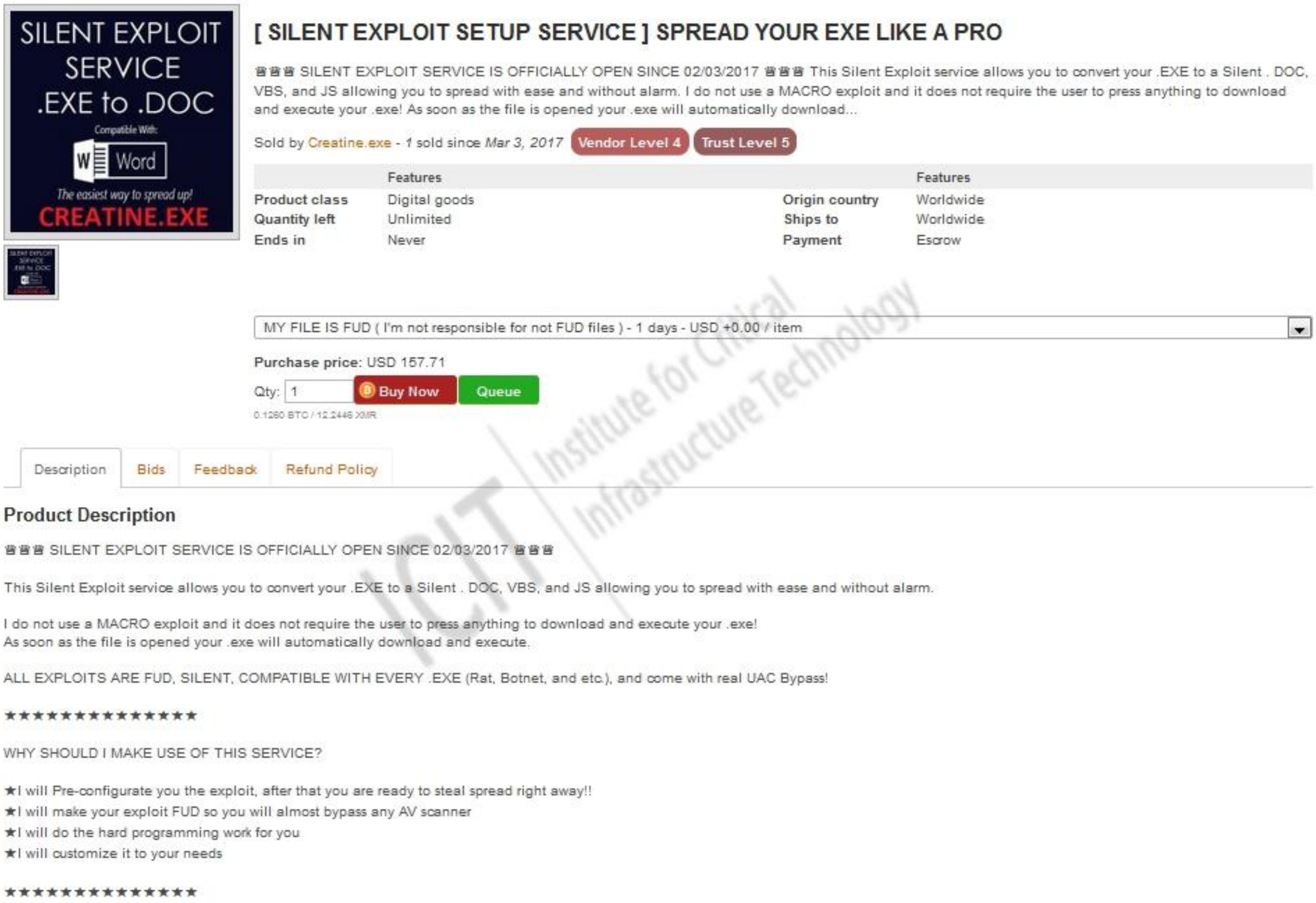
Skyscraper, Jan 6, 2017

Figure 2 captures a "noob" offering to sell healthcare data on Deep Web forums. The data was allegedly obtained from healthcare and dental insurer systems. The unsophisticated attacker (possibly an insider) was able to obtain over 100,000 "fullz" without being a Deep Web insider. The post captures how lax healthcare cybersecurity has become.

For a variety of reasons, over recent years, healthcare data has become increasingly digitized. Though efficiency, accountability, and care have improved as a result, the major downside has been the vulnerability of the data to cyberattack. Hackers target health records for Medicare fraud, identity theft, foreign intelligence, and other purposes. Because the sector lacked adequate cybersecurity and basic cyber-hygiene, EHR and other health data were easy and lucrative targets for even unsophisticated attackers. The stolen data was used to purchase items, to fraudulently apply for, receive, or pay for care, to access prescriptions, or were modified for other purposes. According to a recent Accenture survey, 1 in 4 patients have had their healthcare data stolen and 1 in 2 of those disclosures have resulted in identity theft, costing victims an average out-of-pocket cost of $2,500 per incident. However, as the Deep Web markets saturated, the value of health records diminished and attackers began to look at additional profit streams. Ransomware became an attractive attack vector because it is easy to deploy, healthcare providers often fell victim through basic social engineering, and because it literally weaponized encryption against the very lives of patients and the reputation of the hospital, thereby increasing the victim's willingness to pay [3].

A healthcare breach increases patient churn by 6.7% and results in a reputational loss of nearly $4 million, not counting the estimated $1 million necessary for breach remediation. According to a joint report by Protenus and DataBreaches.net, based on 450 incidents disclosed to HHS, the media, and other sources, 2016 featured at least one healthcare breach per day, affecting more 27 million patient records. The onslaught does not appear to be abating. Protenus found 31 health data breaches, affecting 388,307 patients, in January 2017 alone [3]. Up until now, C-level management and hospital administrative staff have failed to adequately protect healthcare data from exfiltration by domestic and foreign cyber-threat actors. It was bad enough that every time a patient entered the healthcare system, in need of treatment, the provider put them at potential cyber risk. Informed patients had to choose between receiving care and putting their information at risk, or avoiding healthcare providers and suffering the associated adverse implications. Now, ransomware threatens even the basic comfort of knowing that care is available because a single ransomware attack can self-propagate through a healthcare network and render essential equipment non-operational. Worse, ransomware is still developing as an attack vector. Soon it may be able to precision target specialized equipment, infect patient IoT devices, or do much worse. It's time for the health sector to act. The health sector must evolve. The previous excuses for the negligence within the sector range from the incompatibility of systems with modern cyber-defenses, the cost of cybersecurity reform, the lack of dedicated and knowledgeable personnel, the prioritization of patient well-being over security and privacy, etc. Those excuses no longer apply and are no longer sufficient. Artificial intelligence solutions based on machine learning algorithms secure even legacy technology in cost-effective and efficient solutions that seamlessly automate security without requiring the express dedication of on-site personnel.

Figure 3: Exploit Kit Guaranteed to Bypass Traditional Anti-Virus Solutions



[SILENT EXPLOIT SETUP SERVICE] SPREAD YOUR EXE LIKE A PRO

☎☎☎ SILENT EXPLOIT SERVICE IS OFFICIALLY OPEN SINCE 02/03/2017 ☎☎☎ This Silent Exploit service allows you to convert your .EXE to a Silent . DOC, VBS, and JS allowing you to spread with ease and without alarm. I do not use a MACRO exploit and it does not require the user to press anything to download and execute your .exe! As soon as the file is opened your .exe will automatically download...

Sold by Creatine.exe - *1* sold since *Mar 3, 2017* Vendor Level 4 Trust Level 5

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

MY FILE IS FUD (I'm not responsible for not FUD files) - 1 days - USD +0.00 / item

Purchase price: USD 157.71

Qty: 1 Buy Now Queue

0.1260 BTC / 12.2446 XMR

Product Description

☎☎☎ SILENT EXPLOIT SERVICE IS OFFICIALLY OPEN SINCE 02/03/2017 ☎☎☎

This Silent Exploit service allows you to convert your .EXE to a Silent . DOC, VBS, and JS allowing you to spread with ease and without alarm.

I do not use a MACRO exploit and it does not require the user to press anything to download and execute your .exe!
As soon as the file is opened your .exe will automatically download and execute.

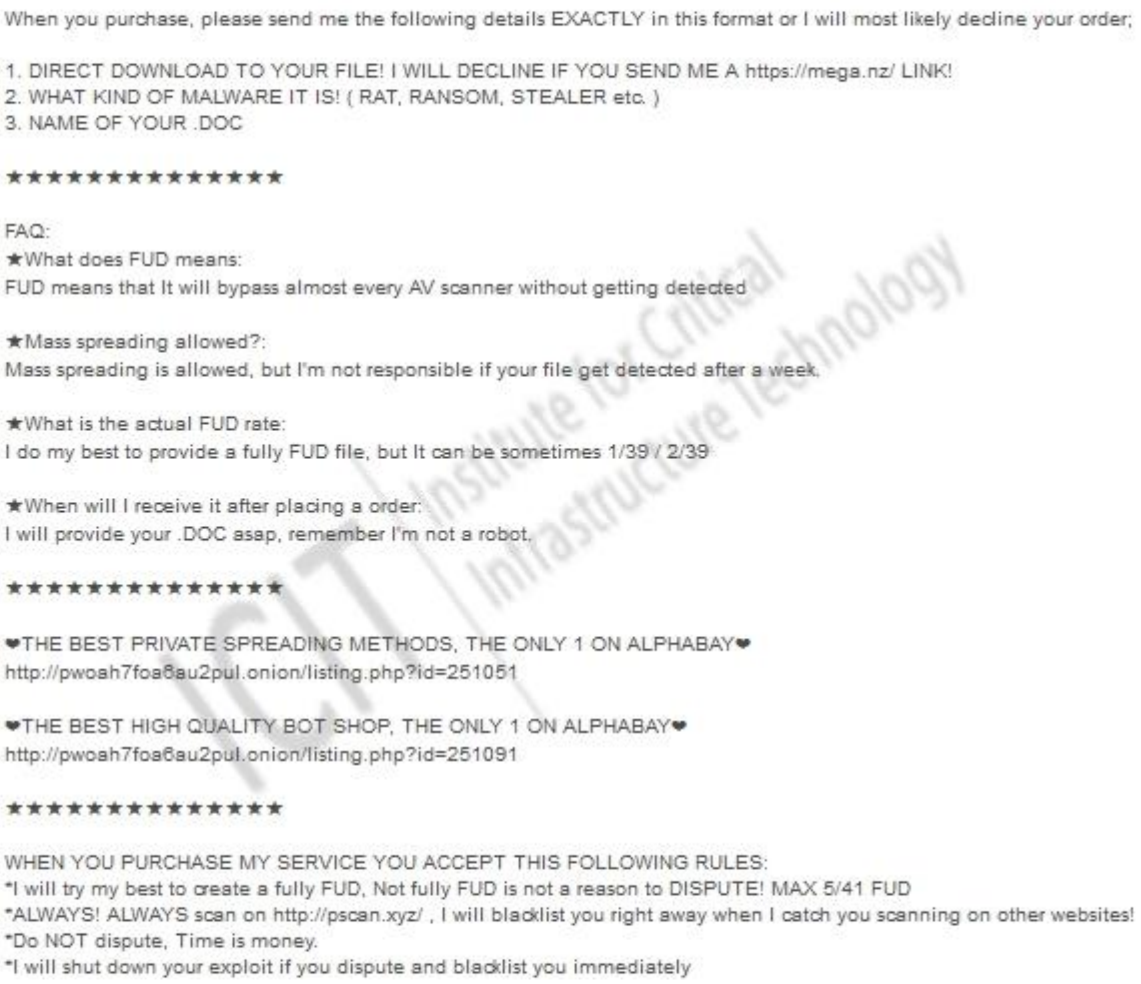
ALL EXPLOITS ARE FUD, SILENT, COMPATIBLE WITH EVERY .EXE (Rat, Botnet, and etc.), and come with real UAC Bypass!

★★★★★★★★★★★★★★

WHY SHOULD I MAKE USE OF THIS SERVICE?

★I will Pre-configurate you the exploit, after that you are ready to steal spread right away!!
★I will make your exploit FUD so you will almost bypass any AV scanner
★I will do the hard programming work for you
★I will customize it to your needs

★★★★★★★★★★★★★★



When you purchase, please send me the following details EXACTLY in this format or I will most likely decline your order;

1. DIRECT DOWNLOAD TO YOUR FILE! I WILL DECLINE IF YOU SEND ME A https://mega.nz/ LINK!
2. WHAT KIND OF MALWARE IT IS! (RAT, RANSOM, STEALER etc.)
3. NAME OF YOUR .DOC

★★★★★★★★★★★★★★

FAQ:
★What does FUD means:
FUD means that It will bypass almost every AV scanner without getting detected

★Mass spreading allowed?:
Mass spreading is allowed, but I'm not responsible if your file get detected after a week.

★What is the actual FUD rate:
I do my best to provide a fully FUD file, but It can be sometimes 1/39 / 2/39

★When will I receive it after placing a order:
I will provide your .DOC asap, remember I'm not a robot.

★★★★★★★★★★★★★★

❤THE BEST PRIVATE SPREADING METHODS, THE ONLY 1 ON ALPHABAY❤
http://pwoah7foa6au2pul.onion/listing.php?id=251051

❤THE BEST HIGH QUALITY BOT SHOP, THE ONLY 1 ON ALPHABAY❤
http://pwoah7foa6au2pul.onion/listing.php?id=251091

★★★★★★★★★★★★★★

WHEN YOU PURCHASE MY SERVICE YOU ACCEPT THIS FOLLOWING RULES:
*I will try my best to create a fully FUD, Not fully FUD is not a reason to DISPUTE! MAX 5/41 FUD
*ALWAYS! ALWAYS scan on http://pscan.xyz/ , I will blacklist you right away when I catch you scanning on other websites!
*Do NOT dispute, Time is money.
*I will shut down your exploit if you dispute and blacklist you immediately

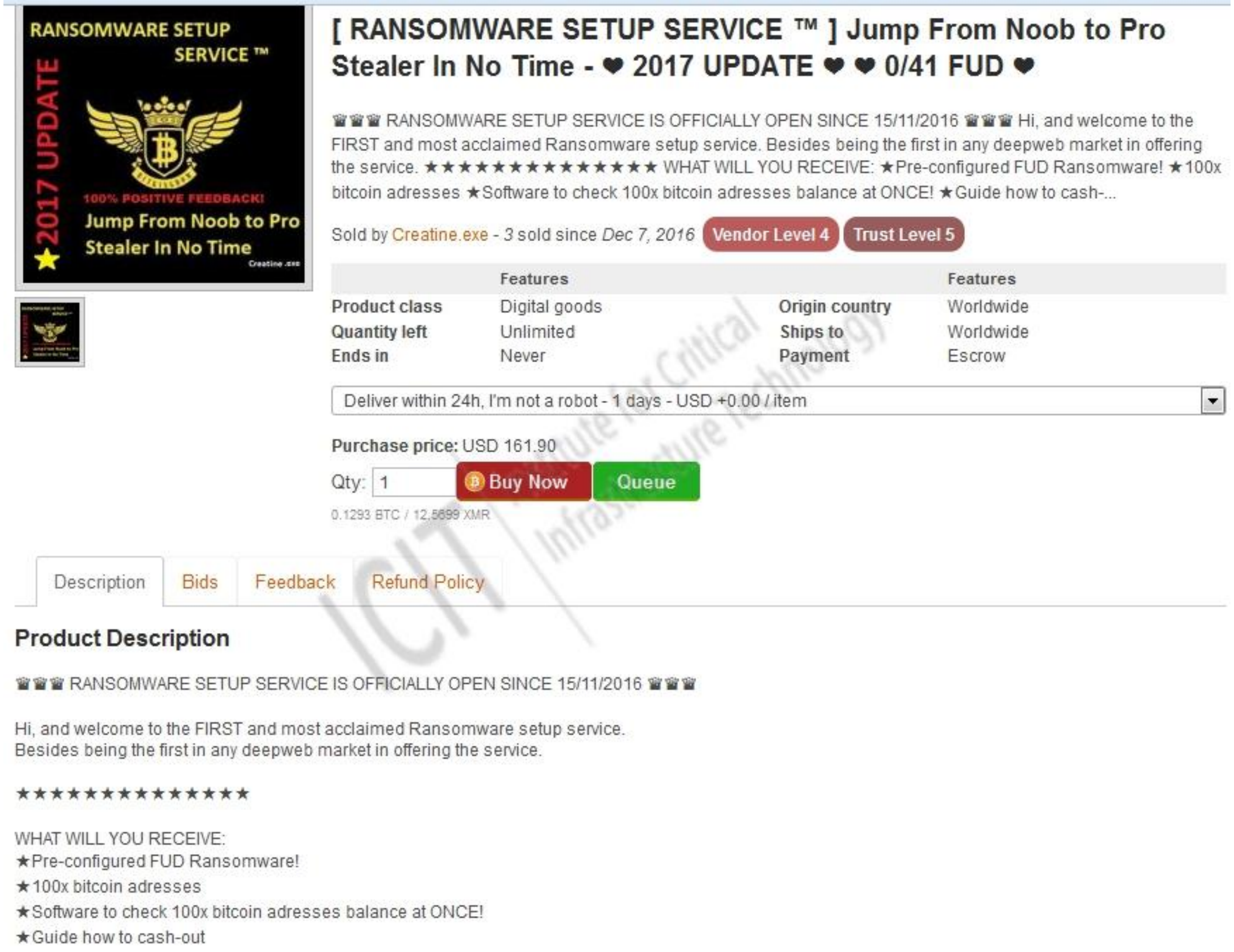
The Silent Exploit service featured in Figure 3 can be used to create malicious documents, images, etc. that bypass conventional security solutions. However, machine learning and AI solutions are sophisticated enough to detect and mitigate threats that use these exploits and attack vectors.

Machine learning is predicted to boost the value of big data, intelligence, and analytics spending to $96 billion by 2021. ABI Research predicts that cyber threats will cause over a trillion dollars in damages to enterprise networks by 2018. Now, it is time for the health sector to ubiquitously apply algorithmic defense technology to cybersecurity. Currently only an estimated seven percent of security professionals claim to use AI solutions in their layered defenses. That rate is expected to increase significantly over the next three years as these powerful solutions become more pervasive, more accessible, and more readily available. These sophisticated defense-grade solutions provide the means for intelligently identifying indicators of cyber threats and automatically prioritizing responses and adapting network defenses to preemptively thwart cyber adversaries. The application of machine learning and artificial intelligence solutions to health IT infrastructures is going to rapidly transform the sector by providing a mechanism through which providers and vendors can protect clinical health data that is stored locally or in the cloud [4]. It is important that during this transformation, healthcare organizations avoid faux experts and that they implement the most sophisticated solutions offered by the most reputable vendors. Cylance's Rob Bathurst, an ICIT Fellow, explains, "Artificial Intelligence and Machine Learning solutions offer many advantages to improve the overall posture of the healthcare sector due to their preventative and predictive nature versus legacy technologies. Healthcare is often searching for better patient outcomes and as those outcomes become more reliant on technology to be sustainable so too must cyber capabilities become preventative versus reactionary. A piece of medical equipment being lost during a procedure due to an inadvertent scan for malware by legacy technology or ransomware infecting the main hospital EMR can not only negatively impact the patient, but may also cause grave harm. One of the largest drawbacks to Artificial Intelligence or Machine Learning solutions in cyber security is that companies must have a good understanding of the problem they're trying to solve and the data they need to solve that problem. Without proper knowledge, planning, and execution AI solutions will often require additional cloud computing resources, potentially expose sensitive files for analysis by their solution, or require a host of compensating technologies for low efficacy models. Artificial Intelligence is not the panacea or the solution to all problems in healthcare with regards to cyber security, but highly focused applications of Machine Learning can result in a much greater protection for organizations and patients."

Algorithmic defenses will improve healthcare cybersecurity by automating network cybersecurity operations in response to learned hacker behaviors. Machine learning and artificial intelligence solutions will soon be the new norm in defense-grade cyber defense because they displace legacy defenses, such as traditional signature and heuristic driven antivirus and because they go beyond Security Information and Event Management (SIEM) solutions. Currently, SIEMs, which aggregate event data from solutions across an IT infrastructure and which attempt to conduct near-real-time security analytics and threat detection, are plagued by data overload, false positives, and false negatives. Algorithmic defense solutions are capable of monitoring every aspect of the network and can automatically do so at rates and accuracies far greater than that of staff. Deep learning algorithms and user and entity behavioral analytics (UEBA) solutions can already incorporate SIEM data and log-based methods to detect and mitigate breaches that result from human-error and insider threat. Machine learning and artificial intelligence solutions dynamically detect and respond to these attacks before adversaries impact systems or operations.

Hospitals are targeted with roughly 88% of all ransomware attacks. Ransomware is used as either a direct revenue stream (the attacker is dependent on the ransom) or as an indirect/ diversionary vector (the attacker uses the ransomware as a distraction and exfiltrates sensitive data amid the panic). Hospitals are particularly vulnerable to external threat actors because they rely on systems that feature more entry and pivot points for cybercriminals to exploit [5]. The modern lethargic cybersecurity of healthcare organizations is not sustainable and is as much to blame for harm to patients as the attacks of cybercriminals. Algorithmic defense solutions may be the only solution capable of remediating the vulnerabilities of the sector and mitigating the harms poised to physically and financially cripple patients. In demonstration, consider that ransomware disproportionately targets the healthcare sector. Also consider that in addition to financially impacting the organization, with no guarantee that systems will be decrypted, ransomware also prevents critical healthcare systems from serving patients. Even an administrative PC, if located in a critical location, such as the emergency room, and infected with ransomware, can pose a major harm to health and human safety. Attacks on email and messaging systems may result in more significant impacts.

Figure 4: RaaS and Setup Services Enables Unsophisticated Attackers to Target Healthcare Organizations


RANSOMWARE SETUP SERVICE ™
2017 UPDATE
100% POSITIVE FEEDBACK!
Jump From Noob to Pro Stealer In No Time
Creatine.exe

[RANSOMWARE SETUP SERVICE ™] Jump From Noob to Pro Stealer In No Time - ❤ 2017 UPDATE ❤ ❤ 0/41 FUD ❤

♛♛♛ RANSOMWARE SETUP SERVICE IS OFFICIALLY OPEN SINCE 15/11/2016 ♛♛♛ Hi, and welcome to the FIRST and most acclaimed Ransomware setup service. Besides being the first in any deepweb market in offering the service. ★★★★★★★★★★★★★★ WHAT WILL YOU RECEIVE: ★Pre-configured FUD Ransomware! ★100x bitcoin adresses ★Software to check 100x bitcoin adresses balance at ONCE! ★Guide how to cash-...

Sold by Creatine.exe - *3* sold since *Dec 7, 2016* Vendor Level 4 Trust Level 5

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Deliver within 24h, I'm not a robot - 1 days - USD +0.00 / item

Purchase price: USD 161.90

Qty: 1

0.1293 BTC / 12.5699 XMR

Product Description

♛♛♛ RANSOMWARE SETUP SERVICE IS OFFICIALLY OPEN SINCE 15/11/2016 ♛♛♛

Hi, and welcome to the FIRST and most acclaimed Ransomware setup service.
Besides being the first in any deepweb market in offering the service.

★★★★★★★★★★★★★★

WHAT WILL YOU RECEIVE:
★Pre-configured FUD Ransomware!
★100x bitcoin adresses
★Software to check 100x bitcoin adresses balance at ONCE!
★Guide how to cash-out

Ransomware-as-a-Service and newer Ransomware Setup Services, shown in Figure 4, enable even unsophisticated script kiddies to target healthcare organizations and to inflict harm on patients. Services like these greatly expand the threat landscape and proliferate the number of threat actors.

In demonstration, consider how ransomware impacted the healthcare sector last year. In January 2016, a ransomware attack prevented Titus Regional Medical Center in Mount Pleasant, Texas from accessing its files. In February, Hollywood Presbyterian Medical Center paid $17,000 (40 bitcoins) to end a two-week attack. In the same month, the Los Angeles County health department identified traces of ransomware on five of its systems. The email system of Lukas Hospital and the systems of Klinikum Arnsberg hospital, in Germany, were also attacked in February 2016. Four administrative computers in The Ottawa Hospital were also infected. In March 2016, the Methodist Hospital in Henderson Kentucky lost use of its electronic-based web systems for five days due to a ransomware attack. Ransomware against DeKalb Health in Indiana was harmful enough to disrupt administrative systems and force patient diversion to other hospitals. Hackers who attacked the Kansas Heart Hospital even demanded additional money in order to decrypt critical systems, after the hospital paid the initial ransom. A ransomware attack on Reston, Va.-based Professional Dermatology Care affected approximately 13,237 patient records.

The San Diego Alvarado Medical Center was targeted in March 2016, along with King's Daughters Health in southeast Indiana. MedStar Health in Washington D.C. was locked out of its systems for days. Chino Valley Medical Center in Chino, California, and Desert Valley Hospital in Victorville, California were similarly attacked by hackers demanding a ransom for the release of critical systems. Marin General Healthcare District and Prima Medical Group lost two weeks of clinical information related to nine medical centers, after a ransomware attack forced reversion to a failed backup system; overall, the incident affected 2,292 patients of Marin Healthcare District and 2,934 patients of physicians with Prima Medical Group who work with Marin General Hospital. A ransomware attack against the New Jersey Spine Center in Chatham, N.J. was also reported in July 2016. In August 2016, the Urgent Care Clinic of Oxford Mississippi suffered an attack reportedly from foreign threat actors. Two servers belonging to Keck Medicine in Los Angeles were also infected with ransomware.

Additionally, an August ransomware attack on the Rainbow Children's Clinic in Grand Prairie, Texas affected 33,638 patients and a later investigation proved that a number of patient records were deleted during the incident [6] [7]. In November 2016, the Northern Lincolnshire and Goole NHS Foundation Trust took three hospitals offline due to a Globez ransomware attack [8].These are but a fraction of the total ransomware attacks that impacted the healthcare sector and jeopardized patients' lives and data, in 2016. The attacks above were just a few that were prolific enough to garner media attention. Sources indicate that a greater number of attacks went unreported because the demands were less than the $5,000 threshold required by the FBI for law enforcement intervention and the 500 or more affected records reporting requirement of HHS. Organizations also fear a loss of reputation if incidents were disclosed [6] [7]. Nevertheless, 329 healthcare breaches were reported to HHS in 2016, up from 280 in 2015. In fact, 50 breaches have already been reported in the first months of 2017 [9]. Already in 2017, the largest hospital group in the U.K., Barts Health NHS Trust -- which incorporates five East London hospitals, 15,000 staff, and provides care to millions of patients a year-- was infected with malware and could have just as easily been infected with ransomware [8]. In fact, 88 out of the 260 NHS trusts across England, Scotland, and Wales were the victim of ransomware attacks over the last 18-month period [10].

Attacks against hospitals are not decreasing in frequency or severity. If anything, they are occurring more often as exploit kits, ransomware, and other malware become more available and easier to use. Ransomware-as-a-Service and similar platforms make the healthcare sector a viable and profitable target to even the least impressive script kiddie. This level of exposure and this vulnerable of an attack surface is reprehensible, and it is primarily the result of the negligence, greed, ignorance, and imposed bureaucracy of healthcare executives who refuse to adopt machine learning solutions and other bleeding-edge technologies essential to secure and protect critical healthcare systems from domestic and foreign cyber-threat actors. Machine learning and artificial intelligence solutions capable of detecting and deterring ransomware and other threats exist and are already available from reputable vendors.

Machine Learning in Healthcare Cybersecurity

Pacemakers, insulin pumps, defibrillators, and other medical equipment are extraordinarily vulnerable to cyberattacks. Nothing has been done to prevent hackers from exploiting the historically lax security of embedded devices, medical equipment, and mission critical systems [11]. Lives are at risk, and C-level executives are ignoring potential solutions capable of protecting patients from harm and future exploitation. Many healthcare organizations are actively doing nothing to protect these devices, critical systems, or patient data, from the incessant threat of ransomware and other malware despite the availability of defense-grade artificial intelligence and machine learning solutions capable of mitigating these threats. Up until now, healthcare organizations have dismissed these solutions because they were ignorant of the potential benefits of algorithmic defensive solutions and because patients, politicians, the media, and the community at large were not holding key decision makers accountable for demonstratively securing healthcare data. The sector has become so susceptible to the preponderance of unsophisticated and sophisticated, foreign and domestic cyber threat actors, that patients are desensitized to breach notifications and many healthcare organizations have, negligently and in some cases illegally, stopped disclosing incidents. Each and every health sector payer, provider, and insurer that adopts artificial intelligence and machine learning defense-grade solutions, contributes to repairing the cybersecurity of the health sector; in doing so, they also rebuild the trust between patients and healthcare organizations.

Machine Learning solutions will improve healthcare cybersecurity by enabling solutions that recognize, learn, and adapt to hacker behavior and that automate network defenses [4]. Centrify's David McNeely, an ICIT Fellow, expounds, "There are at least a couple of different ways that machine learning can help to improve the security posture of any organization including healthcare. One of the more well-known uses for machine learning is to help identify anomalous behavior of individuals accessing healthcare infrastructure and applications, these systems will identify patterns of normal usage and alert or flag events that are out of the ordinary. The second use case is to leverage machine learning to calculate a risk score for specific events as they happen based on the similarity or not to the normal behavior observed for the user performing the specific events. Once the risk score has been determined in real-time, the system can use this during a login event to either grant the access for a low-risk event or to challenge for Multi Factor Authentication [MFA] or possibly block the access for high-risk events. In this way, the system enables IT to apply MFA more liberally across infrastructure and applications since the machine learning system will make decisions of risk which determine if MFA will actually be applied or not." Protenus's Robert Lord, an ICIT Fellow, adds, "ML and AI solutions that focus on curbing cyber threats stemming from insider activity, phishing, and ransomware are especially promising. Over 40% of health data breach incidents in 2016 were the result of insider activity. Ransomware caused over 25% of incidents, and phishing served as the gateway for many such incidents. AI and ML solutions that gain a 360 view of how every EHR user interacts with patient data, understand the clinical context surrounding each user access, and transform privacy monitoring from a reactive to proactive process in order to quickly spot behavioral anomalies are keys to improving healthcare cybersecurity."

Currently, AI is benevolently harnessed for network defense; however, there is every indication that adversaries are already attempting to reverse engineer and research AI solutions in order to garner its unparalleled potential. For once, information security professionals have a major asymmetric advantage over cyber-adversaries in their ability to adopt and utilize artificial intelligence and machine learning solutions. However, that advantage will not last. Currently, machine learning and artificial intelligence solutions are the only sophisticated defense against ransomware and tailored malware attacks. Adversaries have an economic incentive to weaponize any and every emerging technology against healthcare and other organizations that are inadequately securing vast treasure troves of sensitive PII, PHI, proprietary data, and other valuable information. The FBI estimates that ransomware attacks alone will cost businesses $2.3 billion over the next three years [12]. Cybersecurity is a perpetual arms war of escalation. New defensive technologies, such as the emergence of artificial intelligence capabilities, necessitate adversarial innovation as much as it does defensive adoption. As more targets adopt sophisticated defenses, such as machine learning solutions, there are fewer vulnerable "lower hanging fruit" organizations for the same number of adversaries to target. Attackers are incentivized to be the first to bypass the latest cybersecurity solution because doing so rewards the attacker with an open season on a plethora of targets who have not already been compromised by other adversaries. The advantageous attacker can charge greater prices for data, exploits, or malware on Deep Web markets and forums or they can sell access-as-a-service. Machine learning solutions are unique amongst cyber defenses in that there are significant resource barriers to entry that forestall adversarial adoption of the technologies and thereby grant organizations that adopt the solutions early the opportunity to outpace cyberattack campaigns. Sophisticated and innovative machine learning and artificial intelligence solutions are available now. Responsible organizations across all critical infrastructure sectors are already adopting these defense-grade solutions and are making their systems less attractive targets to cyber attackers than those of their competitors. It is reasonable to believe and likely that sophisticated adversaries, such as Chinese state-sponsored advanced persistent threats, have already begun attempts to integrate artificial intelligence and machine learning into the next generation of malware. ICIT Fellow Rob Bathurst (Cylance) contends, “While we are not aware of AI being leveraged in malware it is reasonable to believe that advanced threat actors at some point will try to leverage new technologies as a part of their attacks. This is always a part of the evolution threat actors will make but they may start first with trying to attack an AI capability itself in an attempt to find a vulnerability that can be exploited.”

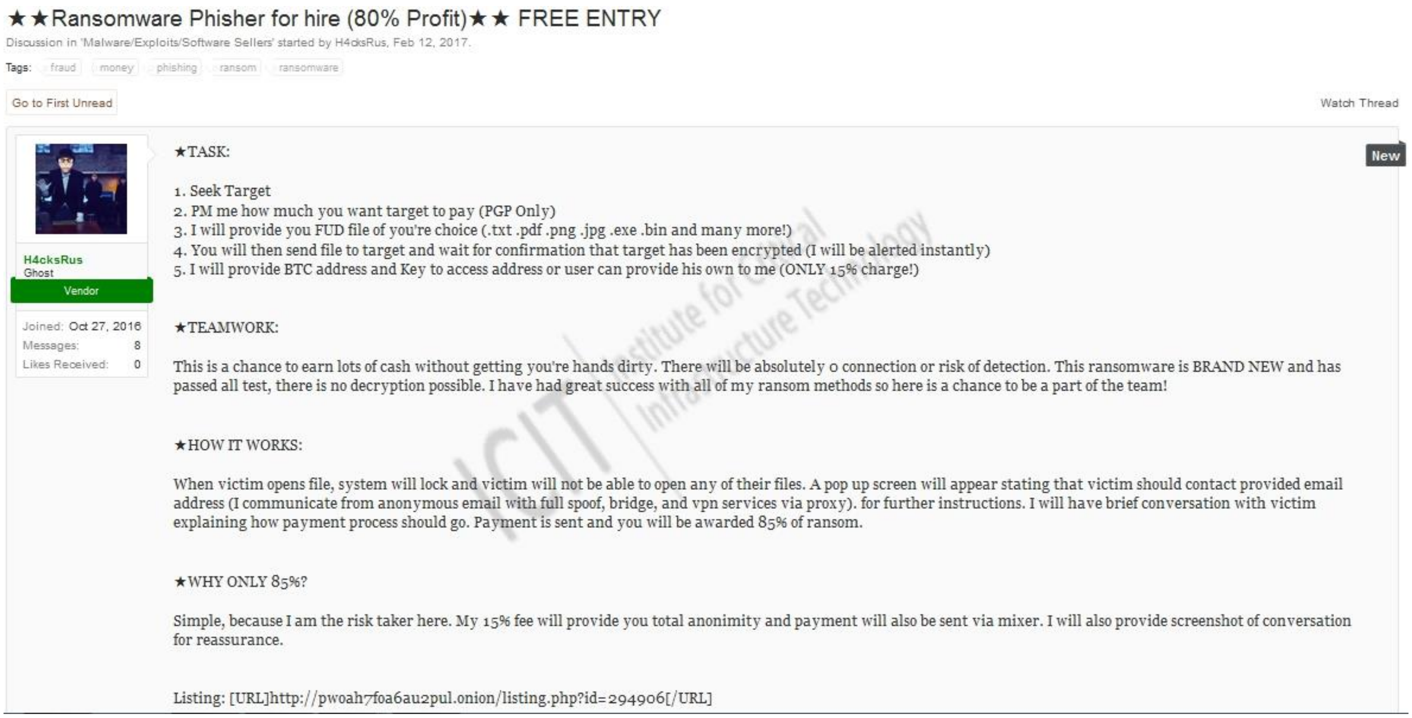
Eventually, even unsophisticated attackers may be able to use AI in smart malware capable of mimicking the mannerisms of known contacts or of spreading through precision tailored lures. Firms that neglect to adopt and implement sophisticated algorithmic defense solutions before widespread adversarial adoption will be devastated by relentless waves of automated precision attacks [12].

Security researchers already developed proof-of-concept AIs designed to besiege employees with multi-vector-social engineering attacks. Healthcare organizations that fail to adopt algorithmic defense –grade solutions will rapidly succumb to an onslaught of sophisticated adversarial campaigns that will eventually incorporate the technology. AI can already be used to write media articles. Soon, adversaries could use it to generate spear-phishing emails and social engineering lures based on the writing style and word choice of specific lure targets. All the malware would need is a writing sample large enough to train the machine learning algorithm and an email spoofing tool. This training selection could be emails, books, lectures, etc. How many employees would open the attachments sent to them from the CEO in an authentic-seeming email? Imagine a ransomware that weaponized sophisticated AI. Such a malware could install itself by dynamically exploiting inherent system vulnerabilities, could self-propagate, remain dormant until specific systems or a specific number of systems have been infected, could obfuscate itself, etc. How devastating could the malware be if it used machine learning techniques to adapt itself in real-time to analysis or decryption efforts? Adversaries may also employ AI to subtly corrupt databases in order to influence business decisions [12]. The simplest such attack, ransomware, weaponizes encryption to stall business operations or to profit from the desperation of victim organizations. Rob Bathurst warns, “We have seen ransomware be developed for specific segments and targets from businesses to individuals to infrastructure. Given the sensitive nature of medical records for celebrities, politicians and business leaders and the competitive IP in the medical industry it is reasonable to expect that the medical segment will see specific ransomware targeted at them being developed.”

Ransomware

While ransomware itself originated in the 1990s, it has re-popularized over the last 18 months [13]. Ransomware attacks profit when victims' need to access the infected system is greater than the fiscal demands of the attacker or the loss incurred due to downtime. The health sector is a prime target for ransomware attacks because every second a critical system remains inaccessible risks the lives of patients and the reputation of the institution. Without immediate real-time access to drug histories, surgery directives, care logs, and other systems, patients suffer and die. Hospitals whose patients suffer as a result of deficiencies in their cyber-hygiene are subject to immense fines and lawsuits. As a result, many healthcare organizations that were targeted with ransomware in 2016 opted to pay for the decryption of their systems rather than suffer a prolonged attack. Further, hospital employees, who are already under significant stress, are not sufficiently trained in cybersecurity or basic cyber-hygiene. Therefore, when a ransomware attack encrypts a medical system, healthcare professionals are ill-equipped to responsibly recognize and mitigate the risk; instead, they willingly succumb to the ransom demands because the monetary demand is typically relatively low compared to the operating cost of the healthcare network [14].

Figure 5: Entry-Level Ransomware-for-Hire Position



★★Ransomware Phisher for hire (80% Profit)★★ FREE ENTRY

Discussion in 'Malware/Exploits/Software Sellers' started by H4cksRus, Feb 12, 2017.

Tags: fraud money phishing ransom ransomware

Joined: Oct 27, 2016
Messages: 8
Likes Received: 0

★TASK:

1. Seek Target
2. PM me how much you want target to pay (PGP Only)
3. I will provide you FUD file of you're choice (.txt .pdf .png .jpg .exe .bin and many more!)
4. You will then send file to target and wait for confirmation that target has been encrypted (I will be alerted instantly)
5. I will provide BTC address and Key to access address or user can provide his own to me (ONLY 15% charge!)

★TEAMWORK:

This is a chance to earn lots of cash without getting you're hands dirty. There will be absolutely 0 connection or risk of detection. This ransomware is BRAND NEW and has passed all test, there is no decryption possible. I have had great success with all of my ransom methods so here is a chance to be a part of the team!

★HOW IT WORKS:

When victim opens file, system will lock and victim will not be able to open any of their files. A pop up screen will appear stating that victim should contact provided email address (I communicate from anonymous email with full spoof, bridge, and vpn services via proxy). for further instructions. I will have brief conversation with victim explaining how payment process should go. Payment is sent and you will be awarded 85% of ransom.

★WHY ONLY 85%?

Simple, because I am the risk taker here. My 15% fee will provide you total anonimity and payment will also be sent via mixer. I will also provide screenshot of conversation for reassurance.

Listing: [URL]http://pwoah7foa6au2pul.onion/listing.php?id=294906[/URL]

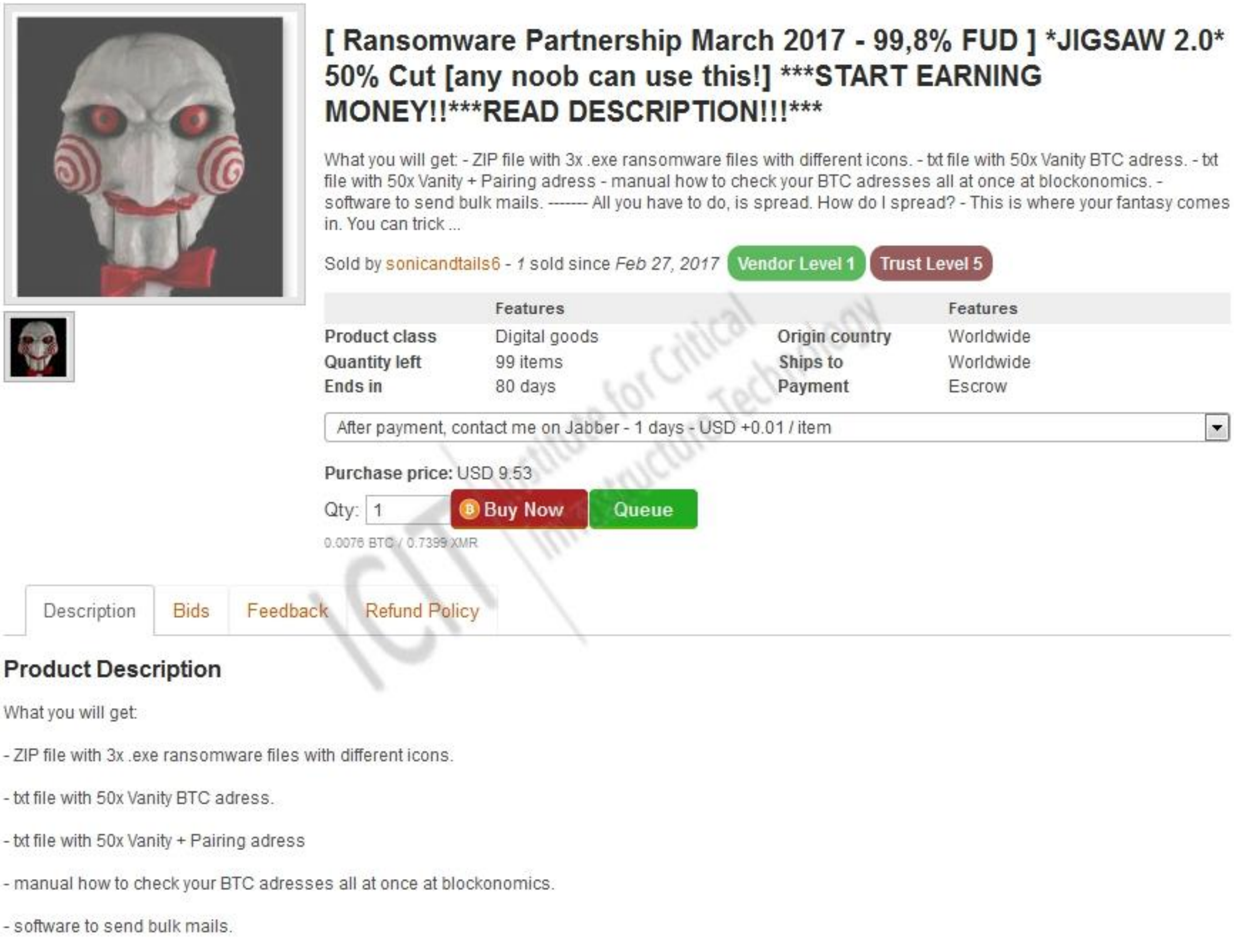
Some attackers, such as the threat actor in Figure 5, expand their operations by hiring or partnering with less sophisticated attackers, who essentially function as employees. These schemes are often aimed at easy, lucrative targets such as healthcare organizations.

Ransomware is unique among malware in that it does not necessarily require stealth; in fact, any attacker attempting to illicit a ransom must make their presence on the system known. High-level attackers use this aspect of ransomware to their advantage by selling or loaning their malware to low-level attackers. As the ransomware becomes more notorious, the high-level developers are able to charge more on Deep Web markets and forums. If security researchers eventually develop an encryption tool on AV signature, then the attackers need only slightly mutate the malware and redistribute it across their service platform. Ransomware-as-a-service schemes, which monetarily and operationally partner unsophisticated script kiddies with more experienced cyber-criminals, have emerged due to the widespread popularity, simplicity, and ease of the attack vector.

Some RaaS require the script kiddie user to split their profits while others require only a subscription fee. Subscription based RaaS are particularly threatening to healthcare and other sectors because they remove the adversary’s fiscal barrier to entry. No longer do wannabe attackers have to purchase expensive malware or invest significant resources. Instead, they essentially loan or borrow the malware. The services, such as the free-commission-based Dot

Ransomware, even provide guides to help low-level attackers get started, to identify targets, and to maximize returns. Dashboards and GUIs included in the malware, enable the unsophisticated attackers to effortlessly monitor multiple infections, to control multiple instances of the malware, etc.

Figure 6: Jigsaw 2.0 FUD RaaS Listing on Alphabay Deep Web Market



[Ransomware Partnership March 2017 - 99,8% FUD] *JIGSAW 2.0* 50% Cut [any noob can use this!] ***START EARNING MONEY!!***READ DESCRIPTION!!!***

What you will get: - ZIP file with 3x .exe ransomware files with different icons. - txt file with 50x Vanity BTC adress. - txt file with 50x Vanity + Pairing adress - manual how to check your BTC adresses all at once at blockonomics. - software to send bulk mails. ------- All you have to do, is spread. How do I spread? - This is where your fantasy comes in. You can trick ...

Sold by sonicandtails6 - *1* sold since *Feb 27, 2017* Vendor Level 1 Trust Level 5

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	99 items	**Ships to**	Worldwide
Ends in	80 days	**Payment**	Escrow

After payment, contact me on Jabber - 1 days - USD +0.01 / item

Purchase price: USD 9.53

Qty: 1

0.0076 BTC / 0.7399 XMR

Product Description

What you will get:

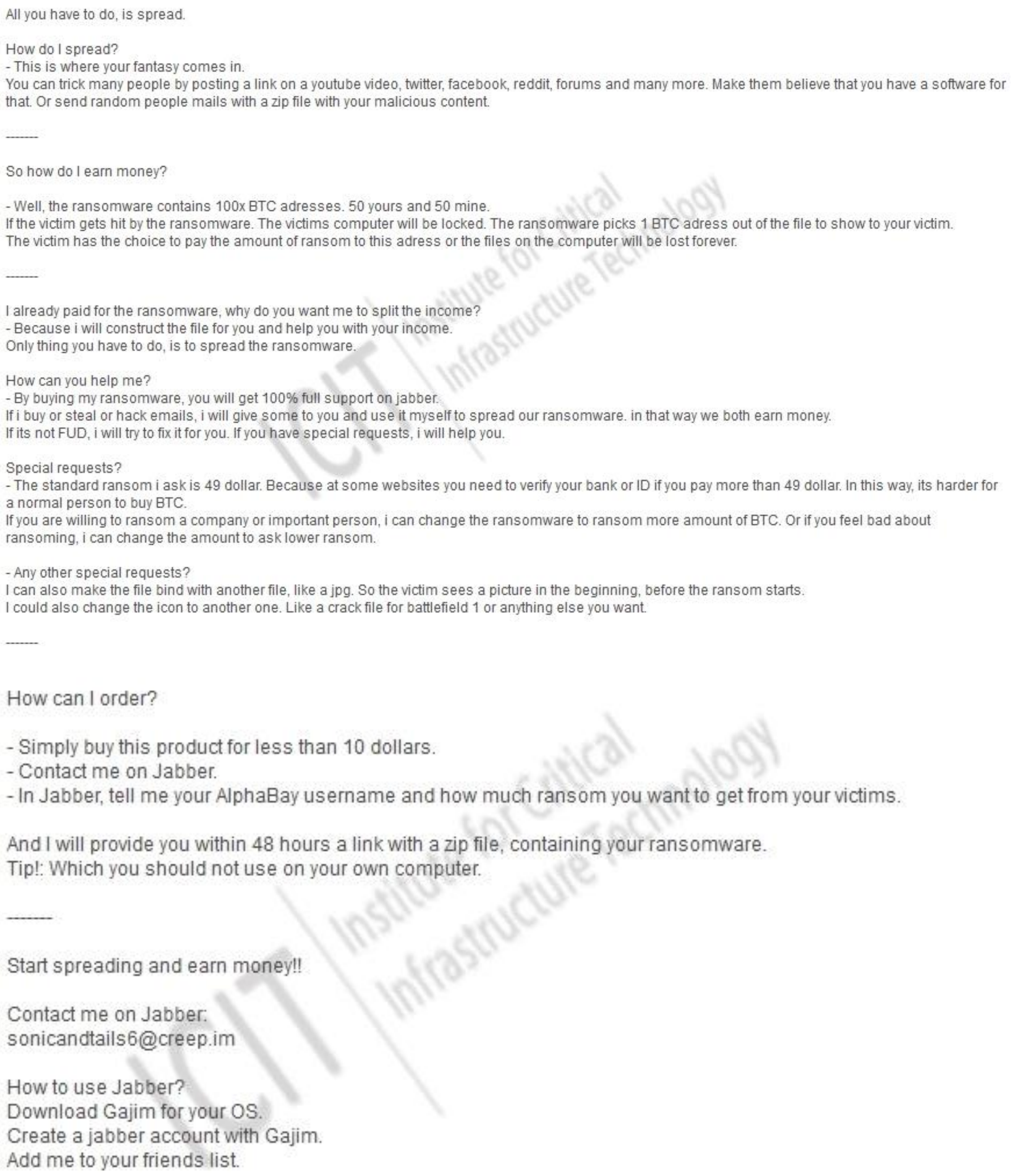
- ZIP file with 3x .exe ransomware files with different icons.

- txt file with 50x Vanity BTC adress.

- txt file with 50x Vanity + Pairing adress

- manual how to check your BTC adresses all at once at blockonomics.

- software to send bulk mails.



All you have to do, is spread.

How do I spread?
- This is where your fantasy comes in.
You can trick many people by posting a link on a youtube video, twitter, facebook, reddit, forums and many more. Make them believe that you have a software for that. Or send random people mails with a zip file with your malicious content.

So how do I earn money?

- Well, the ransomware contains 100x BTC adresses. 50 yours and 50 mine.
If the victim gets hit by the ransomware. The victims computer will be locked. The ransomware picks 1 BTC adress out of the file to show to your victim.
The victim has the choice to pay the amount of ransom to this adress or the files on the computer will be lost forever.

I already paid for the ransomware, why do you want me to split the income?
- Because i will construct the file for you and help you with your income.
Only thing you have to do, is to spread the ransomware.

How can you help me?
- By buying my ransomware, you will get 100% full support on jabber.
If i buy or steal or hack emails, i will give some to you and use it myself to spread our ransomware. in that way we both earn money.
If its not FUD, i will try to fix it for you. If you have special requests, i will help you.

Special requests?
- The standard ransom i ask is 49 dollar. Because at some websites you need to verify your bank or ID if you pay more than 49 dollar. In this way, its harder for a normal person to buy BTC.
If you are willing to ransom a company or important person, i can change the ransomware to ransom more amount of BTC. Or if you feel bad about ransoming, i can change the amount to ask lower ransom.

- Any other special requests?
I can also make the file bind with another file, like a jpg. So the victim sees a picture in the beginning, before the ransom starts.
I could also change the icon to another one. Like a crack file for battlefield 1 or anything else you want.

How can I order?

- Simply buy this product for less than 10 dollars.
- Contact me on Jabber.
- In Jabber, tell me your AlphaBay username and how much ransom you want to get from your victims.

And I will provide you within 48 hours a link with a zip file, containing your ransomware.
Tip!: Which you should not use on your own computer.

Start spreading and earn money!!

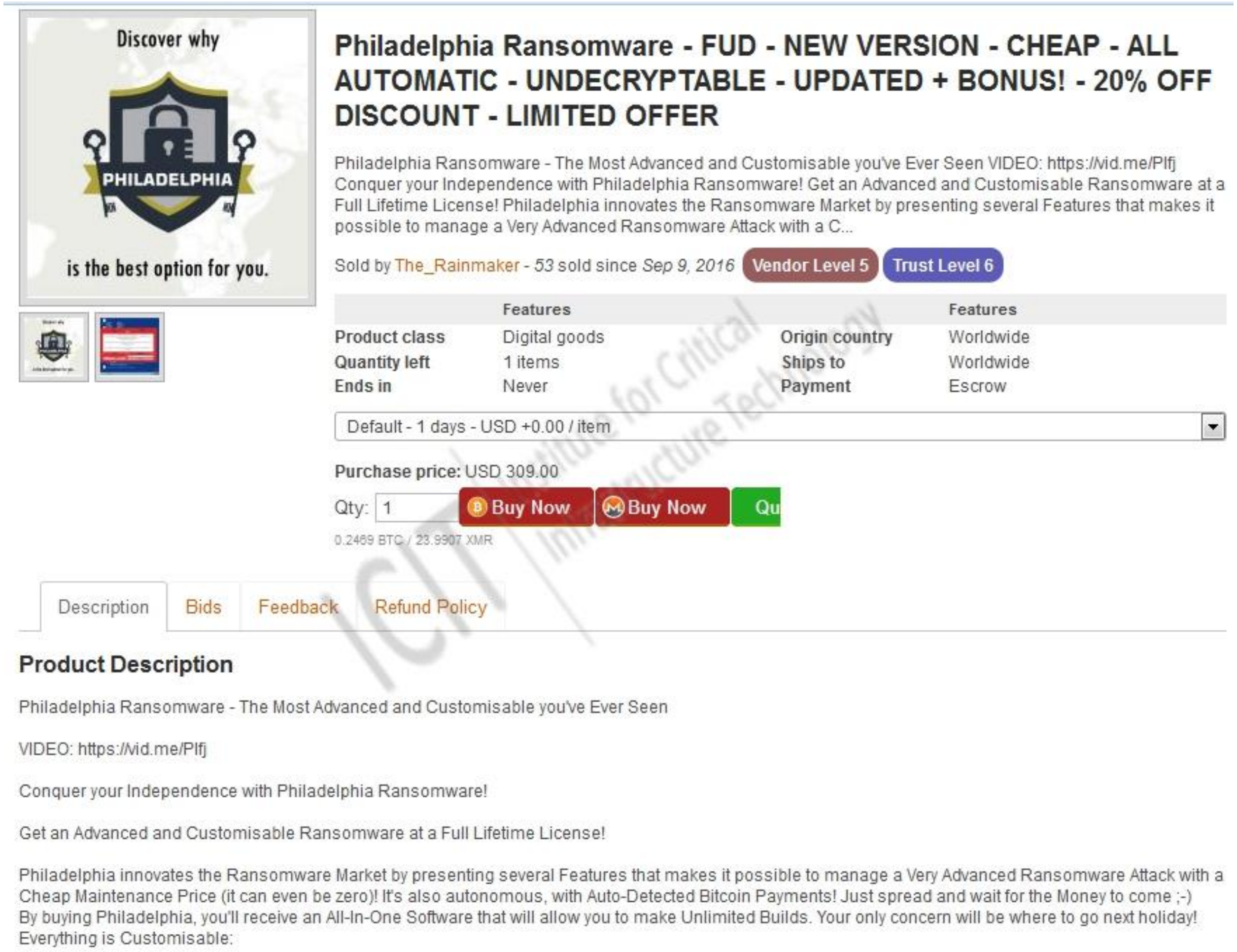
Contact me on Jabber:
sonicandtails6@creep.im

How to use Jabber?
Download Gajim for your OS.
Create a jabber account with Gajim.
Add me to your friends list.

The Jigsaw 2.0 RaaS can be aimed at healthcare organizations by unsophisticated attackers. The author claims that this malware cannot be detected by traditional security solutions; however, the ransomware would be easily detected and mitigated by algorithmic defense solutions.

Most of the ransomware attacks on the healthcare sector in 2016 utilized either the Locky or the Cryptowall ransomware. Now ransomware is evolving. The Samas RansomWorm spreads throughout the entire network, encrypting every server, system, and backup. Front facing servers, which are common in the healthcare sector, are favorite targets. After compromising a machine connected to the corporate domain and establishing a foothold, the attacker steals credentials, identifies target machines via Active Directory (AD) reconnaissance, and laterally navigates throughout the network, infecting each machine with the ransomware. Within one year of targeting the healthcare sector, the Samas group earned $450,000 from the organizations that paid. It is undoubtable that a much greater number of countless other victims refused to pay the ransom and were forced to either revert systems to isolated backups or to suffer the consequences [15].

Figure 7: FUD Philadephia Ransomware



Philadelphia Ransomware - FUD - NEW VERSION - CHEAP - ALL AUTOMATIC - UNDECRYPTABLE - UPDATED + BONUS! - 20% OFF DISCOUNT - LIMITED OFFER

Philadelphia Ransomware - The Most Advanced and Customisable you've Ever Seen VIDEO: https://vid.me/Plfj Conquer your Independence with Philadelphia Ransomware! Get an Advanced and Customisable Ransomware at a Full Lifetime License! Philadelphia innovates the Ransomware Market by presenting several Features that makes it possible to manage a Very Advanced Ransomware Attack with a C...

Sold by The_Rainmaker - *53* sold since *Sep 9, 2016* Vendor Level 5 Trust Level 6

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	1 items	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 309.00

Qty: 1

0.2469 BTC / 23.9907 XMR

Product Description

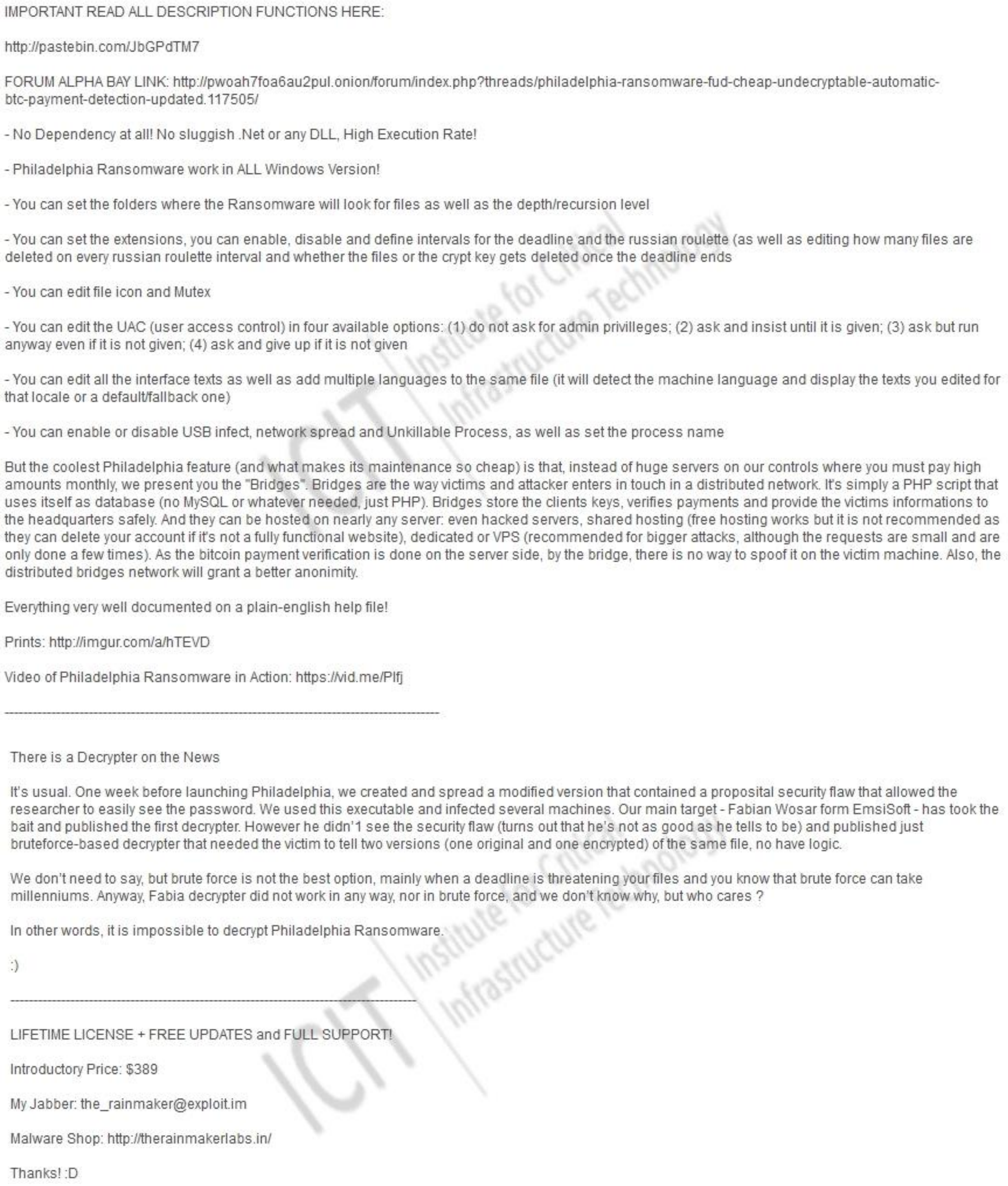
Philadelphia Ransomware - The Most Advanced and Customisable you've Ever Seen

VIDEO: https://vid.me/Plfj

Conquer your Independence with Philadelphia Ransomware!

Get an Advanced and Customisable Ransomware at a Full Lifetime License!

Philadelphia innovates the Ransomware Market by presenting several Features that makes it possible to manage a Very Advanced Ransomware Attack with a Cheap Maintenance Price (it can even be zero)! It's also autonomous, with Auto-Detected Bitcoin Payments! Just spread and wait for the Money to come ;-)
By buying Philadelphia, you'll receive an All-In-One Software that will allow you to make Unlimited Builds. Your only concern will be where to go next holiday!
Everything is Customisable:



IMPORTANT READ ALL DESCRIPTION FUNCTIONS HERE:

http://pastebin.com/JbGPdTM7

FORUM ALPHA BAY LINK: http://pwoah7foa6au2pul.onion/forum/index.php?threads/philadelphia-ransomware-fud-cheap-undecryptable-automatic-btc-payment-detection-updated.117505/

- No Dependency at all! No sluggish .Net or any DLL, High Execution Rate!

- Philadelphia Ransomware work in ALL Windows Version!

- You can set the folders where the Ransomware will look for files as well as the depth/recursion level

- You can set the extensions, you can enable, disable and define intervals for the deadline and the russian roulette (as well as editing how many files are deleted on every russian roulette interval and whether the files or the crypt key gets deleted once the deadline ends

- You can edit file icon and Mutex

- You can edit the UAC (user access control) in four available options: (1) do not ask for admin privilleges; (2) ask and insist until it is given; (3) ask but run anyway even if it is not given; (4) ask and give up if it is not given

- You can edit all the interface texts as well as add multiple languages to the same file (it will detect the machine language and display the texts you edited for that locale or a default/fallback one)

- You can enable or disable USB infect, network spread and Unkillable Process, as well as set the process name

But the coolest Philadelphia feature (and what makes its maintenance so cheap) is that, instead of huge servers on our controls where you must pay high amounts monthly, we present you the "Bridges". Bridges are the way victims and attacker enters in touch in a distributed network. It's simply a PHP script that uses itself as database (no MySQL or whatever needed, just PHP). Bridges store the clients keys, verifies payments and provide the victims informations to the headquarters safely. And they can be hosted on nearly any server: even hacked servers, shared hosting (free hosting works but it is not recommended as they can delete your account if it's not a fully functional website), dedicated or VPS (recommended for bigger attacks, although the requests are small and are only done a few times). As the bitcoin payment verification is done on the server side, by the bridge, there is no way to spoof it on the victim machine. Also, the distributed bridges network will grant a better anonimity.

Everything very well documented on a plain-english help file!

Prints: http://imgur.com/a/hTEVD

Video of Philadelphia Ransomware in Action: https://vid.me/Plfj

----

There is a Decrypter on the News

It's usual. One week before launching Philadelphia, we created and spread a modified version that contained a proposital security flaw that allowed the researcher to easily see the password. We used this executable and infected several machines. Our main target - Fabian Wosar form EmsiSoft - has took the bait and published the first decrypter. However he didn'1 see the security flaw (turns out that he's not as good as he tells to be) and published just bruteforce-based decrypter that needed the victim to tell two versions (one original and one encrypted) of the same file, no have logic.

We don't need to say, but brute force is not the best option, mainly when a deadline is threatening your files and you know that brute force can take millenniums. Anyway, Fabia decrypter did not work in any way, nor in brute force, and we don't know why, but who cares ?

In other words, it is impossible to decrypt Philadelphia Ransomware.

:)

LIFETIME LICENSE + FREE UPDATES and FULL SUPPORT!

Introductory Price: $389

My Jabber: the_rainmaker@exploit.im

Malware Shop: http://therainmakerlabs.in/

Thanks! :D

The Philadelphia ransomware captured in Figure 7 is one of the more sophisticated and rapidly evolving ransomwares on Deep Web markets. It is widely customizable and adaptable against traditional security solutions. More importantly, Philadelphia relies on bridges instead of servers and thereby removes much of the infrastructure barrier-to-entry that deters unsophisticated and low level attackers from entering the market. As similar malware develops (undoubtedly with even more innovative capabilities) it should be obvious to healthcare professionals that machine learning and artificial intelligence security solutions are necessary to detect and mitigate sophisticated ransomware.

Ransomware victims often receive little or no assistance. By law, the FBI does not get involved in such a case unless a $5,000 loss occurs. The U.S. Attorney's Office prefers a $50,000 loss before the FBI dedicates any of its 800 cyber agents; meanwhile, the FBI itself is reportedly reluctant to dedicate resources to an investigation unless there is a potential loss of $100,000 - $200,000. Consequently, if an organization is infected with ransomware, they may not receive assistance from law enforcement if the ransom demand is less than the aforementioned thresholds. Even if the FBI does launch a full investigation into an attack, there is often little that they can do other than assist the victim in rolling back critical systems, provided that systems were adequately backed up [16].

According to the FBI, in the first three months of 2016, ransomware cost victims $209 million. Ransomware results in immediate financial and long-term reputational harm. Worse, if the organization did not adequately backup or protect its data, and if the attacker does not release the data (which is likely) then the data might be exfiltrated or forever lost. While the vast majority of mid-size and large enterprises (250+ employees) have full-time dedicated IT resources, only 17% of small organizations (<50 employees) have full-time dedicated IT resources. Only 15% of small businesses are aware of ransomware threats or the precautionary steps necessary to protect their data and systems. In a recent Malwarebytes survey, 50% of large and medium companies indicated that they had fallen victim to a ransomware attack [17].

The FBI recommends that potential targets of ransomware attacks, such as healthcare organizations, preempt attacks by taking meaningful actions. They recommend that the organization practice proper cyber-hygiene, that they patch and update systems, and that they constantly monitor the modern threat landscape. They advise victims to compartmentalize their network infrastructure in order to limit the spread of malware and to limit the damage of a single breach. Finally, they recommend that the organization have an incident response plan prepared that includes contact with law enforcement. All of these recommendations are foundational cybersecurity; however, they also do little to proactively prevent a breach altogether. The FBI believes that breaches are inevitable. Using traditional responsive cyber-defenses, breaches will occur because people and antiquated technologies will fail. Layered defense-grade cybersecurity solutions, such as artificial intelligence, machine learning, and other algorithmic defenses shift the asymmetric threat landscape to finally reward defenders with a more strategically advantageous posture over the immeasurable hordes of sophisticated and unsophisticated cyber attackers.

Instead of just reacting to threats and in addition to planning incident response, organizations can now use AI and machine learning solutions to proactively thwart adversarial attempts. Healthcare organizations can finally stymie the ransomware epidemic and the plague of PII theft afflicting the sector. These solutions are already available. Vendors handle the implementation and operation of the service at reasonable costs relative to the potential losses. Healthcare providers have no excuse for risking the data and lives of their patients through negligent cyber-hygiene. C-level executives who ignore the advantages of algorithmic defenses and that shy away from early adoption will doom their organizations to be "lower-hanging fruit" than competitors who invest in these innovative solutions now. Algorithmic defense solutions remove the "human error" from cybersecurity and they automate critical security procedures. As a result, if the healthcare sector adopts AI and machine learning solutions, then in time, people may be finally able to trust healthcare providers to "knowingly do no harm" again [16].

IoT devices used in the health and other sectors are unique enough that targeted attacks against them are often not detected by many signature based security solutions. Malware can be easily adapted to target new devices, to have a different or mutagenic signature, or to function differently on different devices. If the device stores or processes enough data, is ubiquitous enough, or if the continued operation of a type of device is mission critical, then a targeted attack is still profitable to a cyber adversary, even if its design necessitates the customization of a malware or an attack vector. Many healthcare IoT devices (insulin pumps, pacemakers, etc.) lack the native security by design or even the local resources to host a security application. For instance, most pacemakers do not encrypt connections or data because dedicating the computational resources to do so reduces the battery life from years to weeks. A ransomware infection, whether intentional or accidental, on a pacemaker, could kill the patient by inadvertently overexerting the resources. Similar attacks on insulin pumps, MRI machines, and other medical devices can likewise threaten patient lives. Machine learning solutions can be used to defend the network against adversarial intrusion and to secure these vulnerable devices by establishing and monitoring a baseline of normal device behavior. If device exhibit uncharacteristic activity, then action can automatically be taken before lives are threatened [18].

The Future of Algorithmic Defenses

At a March 2017 cybersecurity conference in Boston, FBI Director James Comey said, "Healthcare enterprises face all the same challenges that the rest of us do, but a recent plague is one for them to focus on, and that is the ransomware plague, hackers suddenly see the healthcare sector as a piggy bank." The healthcare sector faces a number of challenges including a shortage of information technology and information security talent. Small and medium organizations and those in rural areas are uniquely inadequately secured. A recent report from the HHS cybersecurity task force found that three-fourths of healthcare providers in the country, mostly small and medium providers in rural areas, did not have a single cybersecurity employee [9]. Artificial intelligence systems will not remove the need for qualified cybersecurity personnel, but if implemented across the sector, AI and machine learning solutions will significantly alleviate the talent shortage by automating many cybersecurity and cyber-hygiene functions and by acting as a smart defense component that is capable of recognizing and identifying threats, of discovering and mitigating or patching vulnerabilities, and of managing and regulating user access. The automation and implementation of these functions will allow healthcare networks to deploy qualified personnel and sophisticated defense systems to smaller hospitals and healthcare sites within the network. As a result, each healthcare network will be protected downstream, smaller and less resourced facilities will be secured against targeted lateral attacks, and the cybersecurity of the sector will vastly improve.

Depending on the size of the organization, healthcare cybersecurity may be severely limited by available resources. DLT's Don McLean, an ICIT Fellow, explains, "In healthcare, funding deficiency stems from a natural and understandable emphasis on protecting flesh-and-blood patients rather than bit-and-bytes data. If a hospital administrator has limited funds, and needs to choose a new DLP system to protect data or a new defibrillator to rescue dying patients, they'll pick the latter every time – and they should. 'Your loved one is dead, but his data's safe and sound': no one should ever hear that message.” While small and medium providers can claim that they lack the resources to implement AI, large healthcare networks cannot. Large healthcare providers often suffer when smaller providers are targeted, and now it is time that they take sufficient measures to protect and alleviate the threat to patients and smaller organizations by adopting sophisticated algorithmic defenses. Small hospitals are often downstream targets because they rely on insecure, indefensible, and unpatched systems that lack proper segmentation and isolation. These vulnerabilities in healthcare systems and medical devices are not mitigated because the organizations lack the knowledge or resources to do so. Consequently, larger hospitals and healthcare providers may be laterally compromised. Large health sector organizations can act as early adopters of algorithmic cyber defense solutions; thereby, facilitating the further development of the technology and contributing to its increasing cost efficiency. Further, qualified personnel will be enabled to protect downstream facilities in desperate need of cybersecurity personnel. Qualified information security personnel and sophisticated AI solutions from reputable vendors can patch, secure, and isolate critical systems before adversaries can exploit a vulnerability.

Within the next five years, machine learning solutions will completely supplant Security Information and Event Management (SEIM) and traditional heuristic and signature based anti-virus (AV) solutions. Some even expect SEIM log-based methods to be separated altogether and integrated into User and Entity Behavioral Analytics (UEBA), unsupervised, and deep learning systems; whereas, elements of signature-based AV will be included in only a subsection of supervised machine learning models [20]. Machine learning is currently used to significantly improve the exchange of data and to monitor transactions in the financial sector [19]. The same operations can be undertaken in the healthcare and other sectors. Algorithmic defenses can automatically and seamlessly decide when to implement extra layers of security, such as multi-factor authentication, and can assist in risk assessment and vulnerability mitigation efforts through the application of offensive artificial intelligence.

For instance, machine learning can be used to efficiently facilitate the implementation of blockchain technology. Blockchain is based on the exchange of data between nodes (users, organizations, etc.) via a shared database without the inclusion of a third-party data controller or information silo. Blockchain technology leads to a trusted history of transactions between data shareholders. The goal of blockchain technology is to be scalable, secure, and efficient [2].

The Food and Drug Administration (FDA) is collaborating with IBM's Watson AI division to research the application of blockchain technology to the exchange of owner-mediated data from sources including electronic health records (EHRs) clinical trials, genomic data, health data collected from mobile devices, from wearables, and from IoT devices. The collaboration is focused on the study of how healthcare organizations can leverage massive volumes of disparate and diverse data to improve public health and to assist in new discoveries, through a secure owner-mediated data sharing ecosystem [2].

Machine learning and artificial intelligence will help medical organizations sift through, utilize, and secure the vast amount of data collected via networked mobile systems and other IoT devices. Blockchain can potentially securely connect and standardize fragmented data from across disjointed architectures while empowering each patient to be the primary custodian of their EHR, instead of dozens of organization databases. It provides patients the opportunity to access their personal health information (PHI) and it facilitates sharing that data with choice healthcare providers through a secure channel. Meanwhile, healthcare organizations can share data without blindly trusting the security of third-parties. Further, the unalterable audit trail of transactions holds all stakeholders responsible and accountable for the data during their portion of the exchange process [2].

Barriers to Adoption

C-level executives who lack the knowledge of the capabilities of algorithmic defense solutions or that negligently are not willing to protect healthcare data according to its value and potential for harm if exfiltrated will be the greatest barrier to the ubiquitous adoption of artificial intelligence and machine learning solutions. ICIT Fellow Rob Bathurst (Cylance) agrees and believes that these problems can be addressed. He states, "The largest obstacles to adoption of

Artificial Intelligence/Machine Learning solutions in the healthcare space is often due to a lack of knowledge in the problem space and lack of knowledge of the specialized operating requirements in healthcare. No two healthcare organizations are the same when it comes to their technology stack and their cyber security strategy. The best way to surmount these barriers is for solution providers with strong Artificial Intelligence/Machine Learning products to have internal knowledge of healthcare operations and partner with complex healthcare providers to vet the solution across their enterprise. If a solution is only able to address the needs of core IT, it may miss protecting a much larger segment of non-traditional IT systems such as medical devices and building control systems.”

Conclusion

There's a compounding and unraveling chaos that is perpetually in motion in the Dark Web's toxic underbelly. Forums and marketplaces where exploit kits, ransomware, and other malware are bartered allow for anyone, for any reason, to liberate and unleash one’s sinister urge upon millions of unsuspecting cyber hygienically apathetic organizations and citizens. Code and technology are the new munitions; email and social media are the new weaponized delivery systems. Ransomware, weaponized encryption, allows even the most novice of adversaries to wreak havoc and imprison the data of those people and organizations who have yet to learn the cardinal rule of techno-surviving in this digital age, "Think before you click." Cyber hygiene, patching vulnerabilities, security by design, threat hunting and machine learning based artificial intelligence are mandatory prerequisites for cyber defense against the next generation threat landscape.

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

[1] Scott, James and Drew Spaniel. "The ICIT Ransomware Report: 2016 Will Be The Year Ransomware Holds America Hostage". ICIT. N.p., 2017. Web. 7 Mar. 2017. http://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report2.pdf

[2] O'Dowd, Elizabeth. "IBM Watson, FDA Collaborate On Healthcare Blockchain Research." HITInfrastructure. N.p., 2017. Web. 7 Mar. 2017. http://hitinfrastructure.com/news/ibm-watson-fda-collaborate-on-healthcare-blockchain-research

[3] "Summary Of January 2017 Healthcare Data Breaches Released". HIPAA Journal. N.p., 2017. Web. 11 Mar. 2017. http://www.hipaajournal.com/summary-january-2017-healthcare-data-breaches-released-8690/

[4] O'Dowd, Elizabeth. "How Machine Learning Can Improve Healthcare Cybersecurity." HITInfrastructure. N.p., 2017. Web. 7 Mar. 2017. http://hitinfrastructure.com/news/how-machine-learning-can-improve-healthcare-cybersecurity

[5] Green, Max. "Hospitals Are Hit With 88% Of All Ransomware Attacks". Beckershospitalreview.com. N.p., 2017. Web. 11 Mar. 2017. http://www.beckershospitalreview.com/healthcare-information-technology/hospitals-are-hit-with-88-of-all-ransomware-attacks.html

[6] Dietsche, Erin. "12 Healthcare Ransomware Attacks Of 2016". Beckershospitalreview.com. N.p., 2017. Web. 11 Mar. 2017. http://www.beckershospitalreview.com/healthcare-information-technology/12-healthcare-ransomware-attacks-of-2016.html

[7] "Ransomware: See The 14 Hospitals Attacked So Far In 2016". Healthcare IT News. N.p., 2017. Web. 11 Mar. 2017. http://www.healthcareitnews.com/slideshow/ransomware-see-hospitals-hit-2016?page=13

[8] Palmer, Danny. "'Previously Unseen' Malware Behind Cyberattack Against UK's Biggest Hospital Group | ZDNet". ZDNet. N.p., 2017. Web. 11 Mar. 2017. http://www.zdnet.com/article/previously-unseen-malware-behind-cyberattack-against-uks-biggest-hospital-group/

[9] Chalfant, Morgan. "Health Industry Plays Catch-Up On Cybersecurity". TheHill. N.p., 2017. Web. 11 Mar. 2017. http://thehill.com/business-a-lobbying/323081-health-industry-plays-catch-up-on-cybersecurity

[10] Groucutt, Peter. "Treating Ransomware In The Healthcare Sector". Infosecurity Magazine. N.p., 2017. Web. 11 Mar. 2017. https://www.infosecurity-magazine.com/opinions/treating-ransomware-in-the/

[11] Newman, Lily. "Medical Devices Are The Next Security Nightmare". WIRED. N.p., 2017. Web. 11 Mar. 2017. https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

[12] Sjouwerman, Stu. "AI-Powered Ransomware Is Coming, And It's Going To Be Terrifying". Blog.knowbe4.com. N.p., 2017. Web. 7 Mar. 2017. https://blog.knowbe4.com/ai-powered-ransomware-is-coming-and-its-going-to-be-terrifying

[13] Palmer, Danny. "New Dark Web Scheme Lets Wannabe Cybercriminals Get In On Ransomware - For Free | ZDNet". *ZDNet*. N.p., 2017. Web. 11 Mar. 2017. http://www.zdnet.com/article/new-dark-web-scheme-lets-wannabe-cybercriminals-get-in-on-ransomware-for-free/

[14] Zetter, Kim. "Why Hospitals Are The Perfect Targets For Ransomware". *WIRED*. N.p., 2017. Web. 7 Mar. 2017. https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

[15] Seals, Tara. "Samas Ransomworm Snakes Through Whole Domains". Infosecurity Magazine. N.p., 2017. Web. 11 Mar. 2017. https://www.infosecurity-magazine.com/news/samas-ransomworm-snakes-through/

[16] Sjouwerman, Stu. "Tampa FBI: Your Business Is Going To Get Hacked (Or Get Infected With Ransomware)". Blog.knowbe4.com. N.p., 2017. Web. 7 Mar. 2017. https://blog.knowbe4.com/tampa-fbi-your-business-is-going-to-get-hacked-or-get-infected-with-ransomware

[17] "Monstercloud - Survey Shows Small Biz Most Vulnerable To Ransomware Attacks". ValueWalk. N.p., 2017. Web. 11 Mar. 2017. http://www.valuewalk.com/2017/03/small-biz-ransomware-attacks/

[18] Madhavan, Suresh. "AI, Blockchain, Machine Learning And The Future Of Fintech". Verizonventures.com. N.p., 2017. Web. 7 Mar. 2017.

http://www.verizonventures.com/blog/2016/12/ai,-blockchain,-machine-learning-and-the-future-of%C2%A0fintech/

[19] Buntinx, JP. "Improving Transaction Monitoring With Machine Learning And Blockchain". NEWSBTC. N.p., 2017. Web. 7 Mar. 2017. http://www.newsbtc.com/2016/07/21/improving-transaction-monitoring-machine-learning-blockchain/

[20] "Machine Learning In Cybersecurity To Boost Big Data, Intelligence, And Analytics Spending To $96 Billion By 2021". Prnewswire.com. N.p., 2017. Web. 11 Mar. 2017. http://www.prnewswire.com/news-releases/machine-learning-in-cybersecurity-to-boost-big-data-intelligence-and-analytics-spending-to-96-billion-by-2021-300398664.html