Teaching Case

JITTC

Journal of Information Technology Teaching Cases
2022, Vol. 0(0) 1–11

DOI: 10.1177/20438692211110246
journals.sagepub.com/home/jittc
SAGE

From disruption to ransomware: Lessons From hackers

Pratim Milton Datta[1,2] and Thomas Acton[3]

Abstract

Since 2020, SARS-COV-2 (COVID-19) has forced organizations to pivot towards digital transformation. Yet, the same period has seen a dramatic rise in hacking and ransomware attacks, especially from internationally malicious actors attempting to simultaneously disrupt and profit. Although a knee-jerk reaction has been the adoption of new-fangled technologies as the only way to prevent, detect, and mitigate attacks, this case study highlights how imperative it is for organizations to proactively review and re-engineer their process inefficiencies and human errors as a systematic counter-strategy. Using fictitious characters reflecting real-world hacking processes and outfits, this case projects the need for a new cybersecurity order, where cybersecure process reengineering and human training deserve greater attention than simply investing in newer cybersecurity technologies.

Keywords

teaching case, security, information system ethics, hacking, ransomware, vulnerabilities, process factors, human factors

Characters

Lynn and Mike: Handlers and Senior members of a state-sponsored Cyberhacking agency[1]

Marta: Lead hacker for Fancy Bear, a notorious Cybercriminal hacking outfit

Anders and Karri: Members of Cozy Bear, another notorious Cybercriminal hacking outfit

In the hackers' den

On a crisp but cold morning, Lynn and Mike walked stiffly towards a nondescript boxy building at the edge of the city, their breath fogging ahead of their step. Lynn and Mike were associated with a nondescript group of black-hat hackers selling their services on the dark web, working for various malicious hacking outfits around the world.

At the end of the disheveled gravel street, the building stood, a large concrete box with occasional windows, all shuttered. Grey and unpainted, it spoke to a different time, a time before the world changed. At the entrance stood Marta, finishing her smoke while glancing down at her smartphone. She lifted her eyes, acknowledged Lynn and Mike, briskly snubbed her cigarette, and escorted them into the bowels of the building. Other than scattered cigarette butts littering the doorway, there was little evidence of business within.

Marta led Lynn and Mike to a small, windowless conference room with a rectangular rustic table block, matching chairs, an Ethernet line, and a projector. Marta swiped her keycard, followed by scanning a random QR code on her phone, and let them in! In contrast to the cold corridors, the room was warm from the server cluster in adjacent rooms, all without doorknobs. The walls were clad with soundproofed rough wood panels. A solitary ancient analog phone rested on the table marked with random circular ring stains from years of abuse.

A civilian guard brusquely walked in with a tray of morning refreshments along with a large coffee pot. Without any fanfare, the three quietly poured their coffee.

Marta was one of the brains behind Fancy Bear, a notorious hacking outfit. Lynn and Mike were there to help re-strategize Fancy Bear's cyberattack objectives.

With global governments drafting cybersecurity policies and bolstering security cyber-defenses, black-hat hackers (including ransomware cybercriminals) knew that they were

[1]Ambassador Crawford College of Business, Kent State University, Kent, OH, USA
[2]Department of Management, University of Johannesburg, South Africa
[3]Business Information Systems, J.E. Cairnes School of Business & Economics, NUI, Galway, Ireland

Corresponding author:
Pratim Milton Datta, Ambassador Crawford College of Business, Kent State University, A408 College of Business, Kent, OH 44242, USA.
Email: pdatta@kent.edu

now cybercriminals on the run. By 2021, 80% of global economies (156 countries) had drafted cybercrime resolutions into laws with prosecutable actions (UNCTAD, 2021). Meant to operate in the shadows and never an outfit to seek notoriety, Fancy Bear's exploits and regular media attention were getting too close for comfort. Cyber-legislation was extending its reach, cyber-awareness was building, and targets were learning. Doing business had to change!

The question was, what should be the new cyberattack strategy?

The workings of Fancy Bear

In the mid-2000s, Fancy Bear, also known as APT28, Pawn Storm, and Strontium, inter alia, originated as a state-sponsored "Unit 26165." Since then, Fancy Bear has become a leading state-sponsored cyberespionage and hacking group, responsible for multiple high-profile hacks and attacks.

Fancy Bear's attack vectors (modes of attack) are concentrated, relying primarily on the following

Human Attack: spear-phishing and credential stuffing. Spear-Phishing is a type of phishing attack aimed at a specific target rather than mass targeting. Spear-Phishing attacks aim at injecting malware into a specific, high-value target's computer by luring the target to visit and enter identity and access credentials at malicious sites disguised as legitimate sites.

Spear Phishing attacks are meant to lure specific targets into clicking links and/or downloading malware to reveal important target identity and access credentials (e.g., usernames and passwords). Particularly, identity and access-credentials compromised during spear-phishing attacks are often used for credential stuffing, where compromised username and password combinations are used across multiple sites to gain entry into systems.

Unfortunately, credential stuffing password compromises often originate from simple process and user errors than from deliberate spear-phishing!

One of such process and user errors are system-default usernames and passwords, assigned for user login and registration convenience. Unless users exercise caution and change the default username/password after logging in the system, openly accessible default usernames and passwords become a persistent vulnerability. Hackers can simply reuse system-default access information for *credential stuffing*. And Fancy Bear was deft at figuring out and exploiting this process and user vulnerability.

Process attack: Supply chain attack. A cyber supply chain attack is a cyberattack on specific organizational or software process vulnerabilities withing its information supply chain. Similar to products, software supply chains create a logistics-network of information flows across various vendors, clients, APIs, and open-access protocols across the entire software lifecycle and use. One of Fancy Bear's most prominent supply chain attack was aimed at France's TVMonde5 on 23 January 2015. Fancy Bear Using 7 different modes of penetration, beginning with a process vulnerability exploit. TVMonde5's reporters used a proprietary RDP (Remote Desktop Protocol) to access TVMonde5's broadcast servers. Unfortunately, the server's RDP port access credentials were using the default username. Fancy Bear exploited the vulnerability and used the default credentials, along with spear-phishing, to access TVMonde5's VPN.

With TVMonde5's exposed VPN, Fancy Bear used a Dutch vendor's remote camera control equipment used by TVMonde5. Once Fancy Bear breached the compromised Windows system to create a new administrator-level user with full control of the system. With administrator-level access, Fancy Bear hackers accessed server logs and installed a "logic bomb," a piece of malware code that triggers certain destructive instructions while hidden in the system. Fancy Bear's logic used the firmware log to erase all network switch and router firmware, crashing the networking hardware and causing TV screens to go blank.

Technical attack: Zero-day attack. A Zero-Day attack is a hack attempted on a piece of commercial software code vulnerability during its first (zero-day) and early days of release, before the software developer can discover and patch the vulnerability.

In October 2016, Fancy Bear began a spear-fishing campaign against a series of high-value diplomatic, defense and political targets in the US and Europe. The spear-phishing objective started with an email bait likely to pique interest. The first phishing email spoofed the sender's identity as a legitimate EU Press Officer, with the subject "European Parliament statement on nuclear threats" with a phishing link. The second spear-phishing email contained the subject line "Cyber Threat Intelligence and Incident Response conference" with an infected .doc file attachment.

Once the phishing link or download was clicked or opened, the website or document used its embedded Adobe Flash zero-day vulnerability. The zero-day vulnerability ran a client-side JavaScript component that sent a fingerprint of the target's system configuration back to a command-and-control server. If the target system ran a zero-day (unpatched) Microsoft Windows operating system (Windows Vista to Windows 7) kernel, the malware would infect the target computer, allowing hackers to exfiltrate data from the target computer to predesignated command and control servers.

Fancy Bear used similar zero-day vulnerabilities, in conjunction with human and process inefficiencies, to steal thousands of classified documents from the Democratic National Committee (DNC) networks during 2015 and 2016.

Fancy Bear's attack surface (targets) span the globe, ranging from

Sphere-of-influence attacks. In 2016, Fancy Bear targeted the World Anti-Doping Agency (WADA). World Anti-Doping Agency had recommended Russian athletes be barred from competition in the Olympics that year because of serious doping allegations. Fancy Bear hacked WADA databases and gained access to all competitors' medical information. Fancy Bear released the names of several international athletes that were allowed to compete under exemptions for banned substances, sowing distrust in WADA.

On 19 March 2016, Fancy Bear used spear-phishing using a fake Google security alert message to lure John Podesta, the US Democratic presidential candidate Hillary Clinton's campaign chairman, into compromising his Gmail credentials. Using Podesta's compromised Gmail credentials, Fancy Bear leaked 50,000 of DNC campaign communication emails in October via WikiLeaks. Released just shy of the November US presidential elections, the timing signaled Fancy Bear's intent on swaying public opinion against Hillary Clinton.

Since 2014, Fancy Bear had employed similar realpolitik tactics using a 6-month long spear-phishing of German politicians, intent on swaying voters ahead of Germany's 2017 elections. Fancy Bear continued its spear-phishing and malware attacks on German Marshall Fund, the German Council on Foreign Relations, and the Norwegian Parliament at various intervals into 2020.

Disinformation attacks. Fancy Bear expanded upon the 1923 Stalinist doctrine of "*Dezinformatsiya*" or disinformation, essentially promulgating falsehoods for propaganda and/or detraction. Similar to Datta's (2021) discussion of a *ruse de guerre* in cyberwarfare, Fancy Bear occasioned the use of false flags to sow social and political divisions and fear.

During 2015, at the height of the rise of the Islamic Caliphate, called Daesh or ISIL (Islamic State of Iraq and the Levant), Fancy Bear crated a false flag called "CyberCaliphate" that used social media and spear-phishing to access 5 wives of US military personnel deployed overseas, issuing death threats. In parallel, Fancy Bear initiated a hacking attack under the same "CyberCaliphate" false flag on TV5Monde, the French TV network.

With a growing percentage of worldwide users relying on social media for news, regardless of the veracity of the source, misinformation attacks had become easier.

During an extremely divisive election, while Syldavia was suffering from western embargoes for its military annexation of Crimea in 2014, misinformation attacks became commonplace, aimed at swaying western political sentiment that favored Syldavia. By 2016, Syldavian hackers had employed more than 30,000 automated Twitter "bots" to pump out 1.4 million election-related tweets, meant to influence and misinform. Simultaneously, Syldavian troll armies managed multiple fake accounts, each account anonymously posting, liking, resharing, and retweeting pro-Syldavian and politically divisive articles on social media 50 to 100 times a day.

Critical infrastructure attacks. During the 2014 Russo–Ukrainian military operation to occupy Crimea, Fancy Bear used spear-phishing to infiltrate a Ukrainian military forum. Fancy Bear knew that the Ukrainian artillery used a proprietary program called "ШоШр-Д30.apk" for artillery targeting. Using ШоШр-Д30.apk as a template, Fancy Bear developed the X-agent malware, a combination of remote-access Command-and-Control (C2) and Beacon malware. Fancy Bear's malware exploited Ukrainian artillery electronic targeting systems, compromising Ukrainian artillery positions, and destroying nearly 20% of Ukrainian D-30 howitzers.

The following year, in 2015, an offshoot hacker group, codenamed Voodoo Bear, SandWorm, or APT 74455, launched a successful attack on the Ukrainian power grid. Voodoo Bear hackers penetrated 3 Ukrainian energy distributor systems using BlackEnergy malware, capitalizing on dilapidated, Soviet-era electronic components and poor process controls and checks. Using a combination of Distributed Denial of Service (DDoS) and Ukraine's industrial control system process inefficiencies, the hack resulted in power outages that affected nearly a quarter-of-a-million Ukrainians. Voodoo Bear perpetrated a similar attack on Ukraine's capital city, Kiev's electricity grid in 2016, cutting off electricity to nearly 20% of the inhabitants.

Cozy Bear's hacking strategy

Back in the conference room, Lynn was rifling through her smartphone notes as two fresh faces walked in. Lynn looked up and introduced them to Mike and Marta.

The two new faces, Anders and Karri belonged to another dark-web outfit, referred to, in cybersecurity circles, as APT29 or Cozy Bear.

"Fancy Bear's cyberattacks will be recorded in the annals of cybersecurity as one of the most prolific APT in cybersecurity history! It's now time to join forces…. I

remember your combined 2016 US election cyberhack!" Mike smiled approvingly.

"However," Lynn smiled, "the 2016 US election cyberhack's success was cleverly redundant…don't you think? Sometimes, redundancy is a welcome strategy, especially in hacks!"

"Well," came Karri's rejoinder, "while Fancy Bear used 'X Agent' malware for remote code execution and file transfers, we, at Cozy Bear, used a 'Sea Daddy' malware implant. That way, Cozy Bear could use a PowerShell script to open backdoors to launch malware on an ad hoc basis and compromise various DNC systems."

"Different strategies," Marta from Fancy Bear smirked, "…if one was discovered, the other could remain undetected…clever, don't you think?"

"I agree! Well done!" remarked Mike, "By the way, Cozy Bear's Solarwinds' Orion server hack was brilliant and impressive – western agencies and companies are still reeling from its aftermath!"

"Spelndid, Mike!" answered Marta, with firm conviction. With a hint of pride and arrogance, Marta added "Not just the west but the entire world!"

Anders felt the need to elaborate. He and Marta were core actors in strategizing the SolarWinds' Sunburst hack.

"The world is full of cybersecurity technology vendors selling technology solutions. That makes organizations complacent, assuming that they are secure if they throw money at expensive cybersecurity technologies marketed to look like they are silver bullets. It is that complacency that opens opportunities to capitalize on human and process deficiencies!"

Lynn had been attentively quiet, studiously examining the US NIST's (National Institute of Standards and Technology) NVD (National Vulnerability Database) that identified technical weaknesses for immediate mitigation.

She added, "It's easier to focus on process vulnerabilities than on technology. Companies and white-hat hackers monitor and run penetration tests for report vulnerabilities back to companies. Patches and updates are regularly released as stopgaps to mitigate technology vulnerabilities. But, fixing processes is often overlooked, and people will be people – creatures of habit"

Among the slew of cyberattacks before and during the SARS-COV-2 crisis, the 2020 Solarwinds' Sunburst hack was particularly troublesome! The 2020 Solarwinds' Sunburst hack had infiltrated several high-profile US departments, including the US Department of State, the US Treasury, the Department of Energy, and even the US National Nuclear Security Administration!

The Solarwinds Orion server hack highlighted how even a world-class infrastructure company falls prey to its software supply chain (SSC) process deficiencies.

Cozy Bear hackers exploited two specific SolarWinds' process deficiencies.

"Our Cozy Bear hackers were spot-on!" said Anders. "First, Solarwinds, as a part of its software update process, used the GitHub repository as a collaborative code warehouse. With so much activity, the Cozy Bear hackers realized that Solarwinds' software update process via GitHub was its Achilles' heel!"

Cozy Bear perpetrators used GitHub's misconfigured public code release along with Solarwinds' insecure update server credentials to inject malicious code into a component .dll (a code library) and packaged it in a regular pull-or push based patch update process. And SolarWinds' Orion clients trustingly downloaded and installed the malware.

Marta interjected, "Second, Solarwinds' Orion infrastructure monitoring and management software advised clients to exclude its software from anti-virus and EDR (End-Point Detection and Response) monitoring to reduce Type I errors (false positives from detecting routine activities as threats). This allowed us to infiltrate the Orion gateway itself with the Sunburst hack, compounding the attack surface and establishing a malicious command and control structure!"

"Sunburst hackers capitalized on Solarwinds' software process update inefficiency to inject the trojan (a piece of disguised malicious code) into what looked like an official Solarwinds' Orion server update, the trap was set!"

APTs are particularly adept at leveraging Type I errors by figuring out exact process inefficiencies as the weakest point in the workflow. Once a process weakness is identified, hackers converge on the strike. A technology breach for an automated process inefficiency and social engineering for a manual/human process inefficiency.

"Fancy Bear and Cozy Bear hackers have learned to focus on software process inefficiencies to build its own clandestine command and control spy network," said Marta from Fancy Bear.

Both Fancy Bear and Cozy Bear knew that even the most technical attack capitalizes on human and process inefficiencies as an SOP (Standard Operating Procedure), as Figure 1 depicts.

Graduating to ransomware: A cybercriminal's blue ocean

The guard knocked and entered with freshly brewed coffee and sweet biscuits. As the cups filled with black, aromatic coffee, the group looked edgy. All knew that their discussions were simply a preface to the crux of their upcoming cyberattack strategy.

Lynn spoke, bitingly, "Fancy Bear and Cozy Bear (APT29) know the denouement of our get-together. With more cybercrime legislation being created around the world, hackers need to consolidate their cyberattack efforts with other similar outfits to share best practices. We will lead the way, and set up multi-pronged, coordinated attacks."

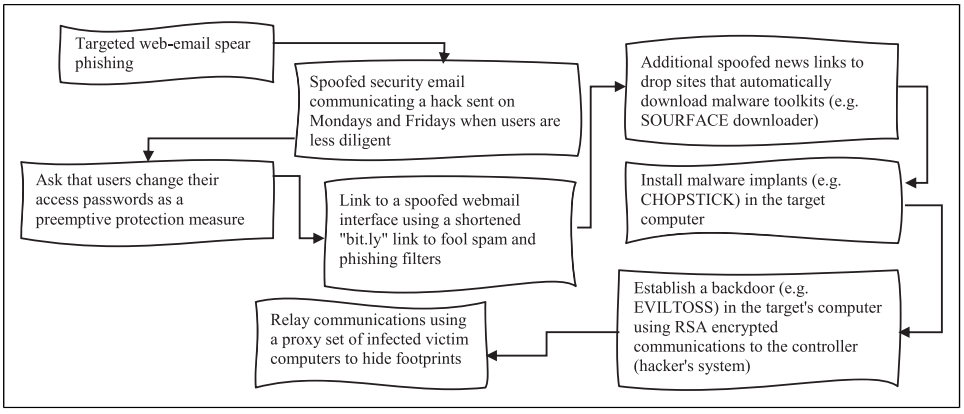

Figure 1. An Example Hacker's standard operating procedure and modus operandi.

"Nothing should be off the menu" added Anders, "from disrupting elections to gain influence and sway realpolitik to taking down civilian and military infrastructures!" Yet unspoken was a palpable call to arms towards a strategic shift.

"Besides, the next round of cyberattacks would not only infiltrate systems but also disrupt them for economic gain, our financial gain!" Mike spoke with a certain terseness "With an unregulated Bitcoin and cryptocurrency craze, Fancy Bear, Cozy Bear, along with other hacking outfits, should also become cyber-privateers! We need to rethink our business model, with the emphasis on 'business'!"

"Indeed! Not so much as to divest from destructive cyberattacks, but to invest and diversify into a more lucrative profiteering endeavor" Marta paused.

"Yes": resounded Karri, "The new weapon shouldn't just be exfiltration but…. Ransomware!"

Ransomware

Ransomware is a malicious software intent on stealing, encrypting, corrupting, and disrupting digital data and systems for ransom purposes, whether to gain extrinsic, financial rewards or non-financial, intrinsic influence.

Ransomware actors include individuals, cybercriminal outfits, and sponsors that encrypt and hold data and/or IT systems hostage until a ransom is paid. Upon receipt of the ransom, ransomware cybercriminals offer a decryption software tool to unlock and regain access to the data or system access.

At the 1988 4th International AIDS conference, when 5.25 floppy disks were in vogue, attendees received an innocuous floppy disk titled "AIDS Info Disk." Once inserted, the AIDS Info Disk, developed by Dr Joseph Popp, an evolutionary Biologist, rewrote the PC boot file, AUTOEXEC.BAT, with its own malicious code. The rewritten file would count the number of PC reboots. Once the number of reboots reached 90, the trojan would hide and encrypt boot directories and activate a message. The message asked the user to pay $189 to a PC Cyborg Corporation in Panama as a prerequisite to rebooting and regaining access to the users' PC. Dr Popp was arrested and claimed that the ransomware was a crusade on behalf of AIDS victims and research.

The "AIDS Info Disk" relied on human fallibility and process efficiencies. Dr Popp knew very well that conference attendees often expected promotional gifts. Conference attendees abandoned caution, allowing for easy circulation within the conference without raising any eyebrows. The label also enticed attendees to open the file in expectation of something free and informative. In fact, the floppy contained one of the earliest trojan ransomware.

The choice of the AIDS conference as an attack surface is akin to a phishing attack, luring victims to a seemingly trustworthy-looking site or venue. Conference attendees assumed that all conference handouts were legitimate. Once lured, Dr Popp's AIDS info disk became the attack vector, rapidly spreading malicious code among unsuspecting conference attendees.

Popp's AIDS info disk ransomware highlighted how even robust technical defenses could fall prey to process and human vulnerabilities—a *modus operandi* that has evolved as a frontline cyberattack tactic.

Dr Popp's ransomware exploited the conference-attendees' interest and appetite for trying out new, untested, and free technologies and software, a human fallibility that has been increasingly abused by ransomware attackers during the SARS-COV-2 crisis.

The SARS-CoV-2 pandemic created newfound opportunities for ransomware actors, exploiting process and security vulnerabilities as organizations pivoted pell-mell to digitally transform their operations—adopting untested technologies on top of unsecure processes and employees lacking cybersecurity training.

Taking advantage of the digital transformation wild west, various ransomware outfits, such as REvil, Conti, Clop,

Netwalker, and DarkSide, emerged, much like terrorist cells, each trying to make a mark by capitalizing on vulnerabilities in technologies, processes, and people!

In a departure from hacks aimed at infiltration and disruption, 2020 experienced a marked increase in Ransomware attacks. According to Reuters (2021), ransomware groups extorted 350 million USD from different companies across the world in 2020.

Many of these attacks capitalized on SARS-COV-2 related work disruptions, from working-from-home, remote server access, unencrypted storage, unprotected WIFI, and unsecured BYOD (Bring Your Own Devices)—with user caution thrown to the wind. Inevitably, 2020 became a ripe time for ransomware attackers.

Ransomware actors

For countries and states in economic turmoil, ransomware actors have burgeoned like privateers in recent years.

Socio-economically, ransomware actors not only brought intrinsic rewards of being able to hack into and disrupt foreign organizations but also brought extrinsic monetary rewards to economically languishing regions. Large sums could be "earned" through reusable boilerplate hacks, with organizations that pay up becoming ever more likely targets to be hit again. Consequently, ransomware groups driving Mercedes G-series wagons in economically depressed areas made joining such groups socially popular, especially among the tech-savvy but disenfranchised youth, or dedicated hackers with nationalistic fervor.[2]

Politically, ransomware outfits attracted a singular patriotic notoriety by disrupting trade among inimical nations, thus securing political capital. In fact, State-sanctioned or state-tolerated outfits adhere to an almost patriotic code of conduct, not hacking allies or fellow citizens, and assisting state intelligence services if asked (Schwartz, 2015).

In short, ransomware socio-economics and politics have allowed ransomware outfits to operate in some of the most prestigious addresses in Moscow City—a financial home to 50 cryptocurrency exchanges implicitly supported by the government and adroit at ransomware money laundering. According to the NY Times (2021), since 2011, US organizations paid $1.6 billion via cryptocurrency ransoms since 2011. In 2020 alone, a ransomware strain called Ryuk extorted an estimated $162 million from encrypting US Hospital computer systems during the pandemic and demanding fees to release the data for Bitcoins or similar (NY Times 2021).

Largely, ransomware has become 21st century privateering (Datta, 2021a; 2021b). During the 18th century and through to the Napoleonic wars, England and France heavily relied on privateers as informal combatants that attacked the enemy on behalf of their respective crowns (countries). French privateers (called *corsaire*) such as Robert Surcouf and English privateers such as Sir Francis Drake attacked each other's merchant ships for prized loot and glory.

Like privateers, some ransomware hackers work under the auspices of the state, albeit at arm's length, under a commission of cyberwar. Their target—organizations. Their motive—profit from ransom from disrupting operations by maliciously encrypting and hijacking data on the cyber high seas!

Of course, hackers followed a strict operational protocol and a hacking code-of-conduct. For example, Russian hackers follow certain rules (Schwartz, 2015):

Rule No. 1: Russians must not hack Russians, or an ally.

Rule No. 2: If a state agency intelligence service asks for your help, you provide it.

Rule no. 3: Hackers must only vacation in countries with on-extradition pacts.

Mike, quietly poring over various digital classified documents, spoke to break the silence.

"Ransomware will include money transfers and following the money will lead to our outfits. We need more cooperation and consolidation to reduce our digital footprints and traceability. Payments can be traced – so we need to shift payments from Bitcoins to more 'hidden' cryptocurrencies such as Monero and/or use privacy wallets such as Wasabi Wallet! Perhaps we need to include Crypto money-launderers! They are called 'Treasure Men' and you can find them on Hydra, a dark web marketplace invisible to search engines!" (Financial Times, 2021)

"Let's learn from mistakes! REvil Sodinokibi encryption malware had a great run for over a year. But a Romanian cybersecurity firm Bitdefender created a free, publicly available decryptor in September 2021 that rendered REvil's Sodinokibi encryption malware useless!"

"And REvil was none the wiser when its ransomware encryptions across many companies were independently decrypted by some 3rd parties. REvil lost more than $500 million in the process." Marta added, "And, as the nail in the coffin, the US FBI, Secret Service, and other global agencies hacked REvil's servers, shutting down REvil's operations."

"Well, Darkside, as a REvil offshoot, took a stealthier approach. Darkside adopted best practices from Cozy Bear's Sunburst hack to try and remain stealthy," remarked Mike.

DarkSide's standard operating procedures (SOP) used:

(i) Software supply chain process deficiencies to access systems via phishing-compromised 3rd party contractor accounts using remote desktop protocols (RDP),

(ii) Bypassed UAC (User Account Control) to hide malware installation that deleted malware footprints,
(iii) Routed RDP commands via port 443 on TOR networks (networks that allow anonymous browsing) to avoid detection
(iv) Like the Sunburst hack, used Cobalt Strike beacon for communications
(v) Used Salsa20 file encryption to encrypt user files and render them inaccessible, and
(vi) Created ransom instructions in a Readme.txt file with
   a. A link to the leaked data on a TOR link
   b. A link to a TOR site instructing payment via Bitcoins or Monero cryptocurrencies
   c. A link to a decryptor that would be made available post-payment.

"What was particularly interesting in DarkSide's *modus operandi*," Lynn riposted, "is how DarkSide promoted its ransomware operations to society!"

DarkSide defended its ransomware hacks not as perpetrators but as egalitarians—modern day Robin Hoods, promising never to hack schools or hospitals but only private companies' profits. DarkSide even posted receipts showing charitable donations from its ransomware to Children International and The Water Project.

"But Darkside gained some unneeded infamy! DarkSide's May 2021 Colonial Pipeline ransomware hack highlighted the devastating effects of a hack on a US energy infrastructure, simultaneous interplaying disruption and privateer-like profit-making. It was tactically sound but a strategic failure!" continued Lynn.

In May 2021, Colonial Pipeline, a large oil distribution company with 5500-mile pipelines connecting southwest US refineries to northeast US gas stations, suddenly shut its operations, leaving gas stations dry. DarkSide had used a compromised employee access password to hack into Colonial pipeline's billing system and encrypt data in order to deny the company access to its customer billing.

DarkSide demanded 75 Bitcoins (around $4.4 million at the time) as a ransom for not releasing the company's private billing information on the Internet and for a decryption key required to restart billing system access. Colonial Pipeline paid up.

"The Colonial Pipeline hack sowed seeds of fear and, suddenly, DarkSide's Robin Hood image fell out of favor." added Mike.

"Eventually," continued Mike, "DarkSide was forced to wrap up its ransomware operations and give up $2.3 million, more than 52% of its gains. The FBI was able to work with international agencies to home in on DarkSide's account and even got a hold of DarkSide's encryption private keys[3] to compromise DarkSide's account and recover funds."

Mike projected a sample of REvil and DarkSide ransomware exploits (Table 1).

Ransomware as a service (RaaS): A new business model

"If we are to match REvil and DarkSide's joint cyberhacks, we have to learn to consolidate or coordinate our own ransomware and other hacking efforts" Lynn deliberated, driving home the point.

"Perhaps, that is where we must think beyond coordination and consolidation." Marta interpolated. "Let's change the business model from Syldavian hacking actors working as independent privateers to Syldavian hackers using Ransomware attacks as a franchise…just like McDonald's and Pizza Hut! See how well they do!"

With more and more digitization and petabytes of data collected, stored, analyzed, and shared every day, data had become an organization's lifeblood. Hackers were building a distributed, deadly business model called Ransomware-as-a-Service (RaaS).

DarkSide was the progenitor of the RaaS concept, interviewing and hiring affiliate hackers (called 26c3weq) to distribute ransomware code for a royalty.

RaaS was truly a franchise business model. RaaS used prepackaged kits and sold them on the dark web, a nefarious, hidden part of the Internet, specifically the world-wide-web, that uses the Tor browser[4] or I2P protocols meant to hide fingerprints and keep it obfuscated from general search engines such as Google. In this Dark Web[5] (or Darknet) replete with dangerous information such as child pornography, prostitution, drugs, extremist videos, drug transaction, terrorism, and even assassins for hire, RaaS kits are commonplace.

RaaS kits were offered via various franchising models. Amateur users, as "script-kiddies" could choose one of various RaaS options:

1. One Time License Fee to use the RaaS kit
2. Monthly subscription model like Netflix
3. Affiliate RaaS program with a monthly fee and approximately 20% in profit-sharing
4. Ad-hoc profit sharing based on the target

RaaS malware sites offer step-by-step instructions on how to run ransomware campaigns (choosing the attack vectors and attack surfaces for maximum damage and leverage), creating ransomware command-and-control infrastructures (e.g., Ranion, Bok, and Raasberry), and ways to collect ransom. Sophisticated RaaS malware sites can also offer custom ransomware toolkits (attack vectors) to

Table 1. Example REvil and DarkSide exploits.

Year (when)	Attack surface organization (who)	Attack vector and strategy (how)	Attack impact (what)
REvil			
May, 2020	US Grubman Shire Meiselas & Sacks (GSMS) entertainment law firm (Paganini 2021)	**Vector**: Ransomware called Sodinokibi encryption malware to lock files. **Strategy:** The ransomware infection was likely perpetrated with insider help, although it is likely that REvil decrypted GSMS' elliptic-curve cryptography to fool detection systems.	756 GB of Donald Trump, Lady Gaga, Madonna, Bruce Springsteen and Elton John data stolen and threatened for public release. $42 million ransom in bitcoin demanded. Payment: Unknown. Likely negotiated with individual clients.
March, 2021	Taiwan's Acer's Microsoft exchange servers (Matthews, 2021)	**Vector**: Zero-day exploit of Outlook web access to compromise Acer's Microsoft exchange servers in India. **Strategy: C**ompromised the exchange server account creation process to scan for and create administrative accounts in vulnerable servers. This created a backdoor to install ransomware malware.	$50 million in bitcoin demanded to recover and return file access. Payment: Unknown. Rejected Acer's $10 million offer.
June, 2021	Brazil's JBS meat-processing systems in the US and Australia (Collier, 2021)	**Vector**: 45 GB operational databases encrypted and data exfiltrated to remote servers. **Strategy:** Possibly from phishing and leaked credentials JBS Australia employees in March 2021.	$11 million in bitcoin demanded. Payment: Paid
July, 2021	Kaseya desktop management software used by over 1,000 companies Lerman and De Vynck, 2021)	**Vector**: Zero-day attack with Kaseya VSA agent hot-fix Malware **Strategy**: Used an authentication bypass vulnerability in the Kaseya web interface. Leveraged supply chain process to push malware to endpoint hosts.	$70 million in bitcoin demanded to restore ransomware encrypted data, forcing severe operational downtime across the world. Payment: Not paid. Used a 3rd party decryptor to decrypt and restore files.
DarkSide			
January-May 2021	47 victims including US: CompuCom IT managed services Canada: Discount car and truck rentals Japan: Toshiba tec. Corp Germany: Brenntag chemicals (Manikanta, 2021)	**Vector**: UAC (user account control) bypass with virtual remote desktop protocols (RDP) routed via port 443 on TOR networks to avoid detection. Cobalt strike beacon for communications and Salsa20 file encryption. **Strategy**: Used cobalt strike beacon malware to open backdoors across vulnerable systems in the vendor's ecosystem and acquire administrative credentials. Encrypted files and locked vendors from being able to access various internal systems, from customer portals	$90 million in bitcoin/Monero ransom demanded Payment: Paid $90 million from at least 47 victims (average of $1.9 million per victim)
May 2021	US: Colonial pipeline shutting down 45% of fuel supply to the US east coast (Turton and Mehrotra, 2021)	**Vector**: Compromised employee access password to hack into colonial Pipeline's billing system. **Strategy**: Used a compromised password secured from the dark web for an active but unused VPN account without any multi-factor authentication process to access the system and remain undetected. Encrypted and denied access to billing system and data.	$5 million in bitcoin ransom demanded. Payment: Paid 75 bitcoins (~$4.4 million), of which $2.3 million was recovered.

Table 2. Example RaaS kits.

RaaS kit demands and sample Victim/s	Attack vector	Strategy
Locky (2016–present), last known to be sold for $3,000 on the dark web. Typically demands bitcoins (0.5 or more). Kentucky-based Methodist Hospital and Hollywood Presbyterian Medical Center	Email attachment with an MS Word document macro. Enabling the macro downloads a trojan malware that changes filenames and encrypts files with *.locky, .zepto, .odin, .aesir, .thor,* and .zzzzz extensions, rendering them unreadable.	Social engineering to find process vulnerabilities with a phishing email message "enable macro if data encoding is incorrect!" Infected users are asked to download the tor browser for anonymous communication, directing them to a ransomware payment website. A decryption private key is offered upon payment.
Philadelphia (2017–present) commonly sold for $400 and based on Stampado RaaS. Typically demands bitcoins (0.3 or more).	Email messages with a false "overdue payment" notice link that contains a Java application for the malware download. The malware encrypts popular filenames into a random alphanumeric name with a *locked* extension with asymmetric (public key) encryption. The malware establishes a PHP bridge between the victim and the command-and-control server to track all communications anonymously.	Social engineering using process and human vulnerabilities. The ransomware infection garbles popular files and creates a LOCKED.txt file. A bitcoin wallet ID is assigned for payment and a deadline timer is created with a Russian roulette feature that randomly deletes user files unless the user pays by the deadline. A decryption PKI key is offered upon payment. Philadelphia RaaS offers a Google maps feature to track victims and payments. The RaaS also offers a "Give Mercy" feature to cancel a ransom demand to protect ransomware criminals from being detected.

serve ad-hoc needs and even specifying how to capitalize on process vulnerabilities, even specifying where to place the malware for a debilitating impact.

Beyond offering RaaS kits on the Dark Web with sites such as "*Hall of Ransom*," hackers invite ransomware affiliates (like franchisees) and target disgruntled employees to launch ransomware attacks against their own companies, offering them a cut of the ransom. RaaS providers often set up production-quality DIY (do-it-yourself) videos and dedicated customer service lines to crowdsource hacks, helping interested affiliates and third-parties walkthrough their targets (attack surfaces), identifying process and human vulnerabilities (Table 2).

Currently, there are multiple RaaS attack vectors in play, each with its unique strategy to capitalize on human and process vulnerabilities. Locky and Philadelphia are examples of two infamous RaaS kits (Baker 2022).

Marta mused, "RaaS kits will open new frontiers and reduce our liabilities and traceability. If we can market RaaS as an enticement to human greed and anti-capitalist sensibilities, we can crowdsource ransomware hacking."

"I agree!" said Lynn. "The next generation of ransomware hacking should focus on coordinating best practices to create RaaS kits that anyone can adopt and let loose with devastating effects. Like DarkSide, we could charge a simple tiered commission, a higher percentage for smaller final ransom payments and a lower percentage for large ransom payments."

Mike spoke, not mincing his words. The day was drawing to a close, and much needed to be done. RaaS offered Lynn and Mike a glimmer of Machiavellian hope.

"We can make RaaS Cybercrime's most despoiling and lucrative franchise. Empower disgruntled and greedy users to take up arms against their own machinery! Our affiliates, sic franchisees, do not even need to know how their RaaS kit works. We will provide them the expertise and teach them how to cover their tracks!" Mike surmised.

Conclusion

It was getting dark and a heavy mist enveloped Ferosimpol." with "It was getting dark and a heavy mist enveloped the city.

As Lynn, Mike, and Marta stepped into the mist ensnaring the dull grey, concrete buildings of the 1970s, unconsciously tucking their heads into their parkas and reaching into their pockets for warmth, they realized how the post-SARS-COV-2 world had ushered in a digitally transformed wild west. Datta (2021c), Datta et al. (2020), Datta et al. (2021), Diffee and Datta (2018)

Companies and countries, like stagecoaches once enamored with new-fangled coach designs but taking the same precarious routes, that is, following age-old inefficient processes, were rapidly adopting digital technologies without changing their business practices—setting themselves up for ransomware pickings. Even the most modern

and armed stagecoach habituated to taking dangerous routes will, sooner or later, get robbed.

Organizations, from businesses to governmental agencies, are often mired into and myopic about buying more cybersecurity technologies rather than fixing their underlying business processes. However, cybersecurity software is merely a lip-service.

Laxities and complacencies in user training and inefficient processes in provisioning critical corporate and public data are an invitation for lurking ransomware actors. Unless businesses fix their processes, even the best security software will fall prey to a bad processes and routines.

The history of falling prey because of inefficient processes and human errors was often drowned by cybersecurity technologies marketing themselves as the next *panacea*. Yet, the Colonial Pipeline ransomware hack or the SolarWinds' Sunburst attack highlighted the need for deliberate process reengineering across the entire software supply chain rather than building siloed technological fortifications.

But there is a reason for such organizational complacencies. It is often easier to invest in technologies rather than reengineer processes. Inefficient, legacy processes are often held sacrosanct. Complacency often rules the roost, because organizations often like the way they "do" or "did" things because they are comfortable with them.

Organizations and users still fail to partition, encrypt, and backup their drives. Users commonly reuse passwords and carry unencrypted USB drives and discarded hard drives with sensitive information. It is normal for most users to access free, unprotected Wi-Fi to access sensitive information and transfer sensitive data, assuming that all cybersecurity onus rests on the organization's IT group. In the ransomware age replete with RaaS kits, a zero-trust environment requires changing our routines; but we and organizations are creatures of habit!

However, hackers and RaaS actors, are, never complacent, constantly sniffing out human- and process-inefficiencies and tweaking their malware payloads for the next zero-day attack or capitalizing on Common Vulnerabilities and Exposures (CVE).

In 1948, freshly emerging from World War II ravages, Sir Winston Churchill addressed the British House of Commons. Paraphrasing the philosopher George Santayana, Churchill said "Those who fail to learn from history are condemned to repeat it."

Our recent cybersecurity history teaches us that overlooking secure process reengineering and user-training is more dangerous than purchasing new cybersecurity technologies! A failure to learn from that history opens doors for CVE threats and a burgeoning RaaS industry.

And that is exactly what cybercriminal outfits counted on!

Individual Discussion Questions

1. What are the differences and motives behind disruption hacks versus Ransomware hacks?
   a. What motivates cyberattackers? Does the motivation differ for state-sponsored cyberhackers, as illustrated in the case?
   b. Can you think of a few disruption attacks and a few ransomware attacks in the past few years? For example, have current global skirmishes and warfare prompted cyberattacks? What can a country do to limit its expose to cyberwarfare?
2. Have cryptocurrencies such as Bitcoins contributed towards increased Ransomware attacks? Why and how? Can Cryptocurrencies also be used to increase transparency? How?
3. Differentiate between Cozy Bear and Fancy Bear. Although their attacks might be slightly different, how does each group leverage process deficiencies? What would you do to mitigate these issues?
4. How does a country's socio-economic condition play a role in ransomware hacking outfits?
5. Explain 3 instances from the case on how process inefficiencies contributed to disruption and/or ransomware hacks!
6. Differentiate between REvil and Darkside and their use of RaaS. Why is RaaS such a dangerous business model?
   a. What would you, as a cybersecurity consultant, do to prevent, detect, and mitigate RaaS-based attacks?
7. If you were managing cybersecurity in a global firm, what would be the 3 most important process and human factors in which you would invest?

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Pratim Milton Datta https://orcid.org/0000-0001-7371-4627

Notes

1. The state-sponsored references are primarily for dramatic effect. Alleged state-sponsorships are anecdotal and there is no confirmed evidence on direct or indirect associations.
2. Similar socio-economic activities include pervasive Somali pirates hijacking merchant ships and sailors in the Horn of Africa or kidnappings in Latin America for ransom.

3. Modern encryption uses a PKI (Public Key Infrastructure) where a pair of keys (one public key and a corresponding private key) are required to encrypt and decrypt.
4. The Tor browser hides all IP addresses (used to locate search origins) by routing them via many proxy servers.
5. Silk Road, one of the first Dark Webs, was a popular site for drug-related transactions. Others, such as Diabolus and Hydra have been seized and shut down. Still, many others remain active and continue to grow.

References

Baker K (2022). *Ransomware as a Service (RaaS) Explained*. Crowdstrike, February 7, url: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

Collier K (2021). *Beef Supplier JBS Paid Ransomware Hackers $11 Million*. NBC News. June 9, url: https://www.nbcnews.com/tech/security/meat-supplier-jbs-paid-ransomware-hackers-11-million-n1270271

Datta P, Walker L and Amarilli F (2020). Digital transformation: Learning from Italy's public administration. *Journal of Information Technology Teaching Cases 10*(2): 54–71.

Datta P (2021a). The promise and challenges of the fourth industrial revolution (4IR). *Journal of Information Technology Teaching Cases*, March. doi: 10.1177/20438869211056938

Datta P (2021b). Hannibal at the gates: cyberwarfare & the solarwinds sunburst hack. *Journal of Information Technology Teaching Cases*, December. DOI: 10.1177/2043886921993126

Datta P (2021c). Cyberruse at the cybergates: technology, people and processes. *ISACA Journal 6*(4): 51–58.

Datta P and Nwankpa J (2021). Digital transformation and pandemic crisis continuity planning during SARS-COV-2. *Journal of Information Technology Teaching Cases 11*(2): 81–89.

Datta P, Whitmore M and Nwankpa J (2021). A perfect storm: psychological and AI (technological) antecedents to information bias anchoring (IBA) in social media news. *ACM Journal: Digital Threats: Research and Practice*. Print.

Diffee E and Datta P. (2018). Cybersecurity: the three-headed Janus. Journal of Information Technology Teaching Cases (Journal of Information Technology *Sister Journal)*, *8*(1), 161–171. DOI: 10.1057/s41266-018-0037-7

Financial Times (2021). The rise of crypto laundries: how criminals cash out of bitcoin. https://www.ft.com/content/4169ea4b-d6d7-4a2e-bc91-480550c2f539

Lerman R and De Vynck G (2021). *Hackers Demand $70 Million to Unlock Businesses Hit by Sprawling Ransomware Attack*. Washington, DC: The Washington Post, July 5, url: https://www.washingtonpost.com/technology/2021/07/05/kayesa-ransomware-70-million-fbi/

Manikanta I (2021). *Ransomware Attack on CompuCom Costs Over $20 Million in Restoration Expenses*. TechDator, March 28, url: https://techdator.net/compucom-ransomware-attack/

Matthews L (2021). *Acer Faced With Ransom Up To $100 Million After Hackers Breach Network*. Forbes, March 21, url: https://www.forbes.com/sites/leemathews/2021/03/21/acer-faced-with-ransom-up-to-100-million-after-hackers-breach-network/?sh=50368ca6750f

New York Times (2021). Companies Linked to Russian Ransomware Hide in Plain Sighturl, December 6th, url: https://www.nytimes.com/2021/12/06/world/europe/ransomware-russia-bitcoin.html.

Osborne C (2021). *Researchers Track Down Five Affiliates of DarkSide Ransomware Service*. ZDNet, May 12. url: https://www.zdnet.com/article/researchers-track-down-five-affiliates-of-darkside-ransomware-service/

Paganini P (2021). *Managed Services provider CompuCom by Darkside ransomware*. Security Affairs, March 5. url: https://securityaffairs.co/wordpress/115300/malware/compucom-darkside-ransomware.html

Reuters (2021). Ransomware attacks soar, hackers set to become more aggressive - Canada spy agency, December 6th: https://www.reuters.com/technology/ransomware-attacks-soarhackers-set-become-more-aggressive-canada-spy-agency-2021-12-06/

Schwartz M (2015). *Russian Cybercrime Rule No. 1: Don't Hack Russians*. Bank Info Security, September 14th: https://www.bankinfosecurity.com/blogs/russian-cybercrime-rule-no-1-dont-hack-russians-p-1934

Turton W and Mehrotra K (2021). *Hackers Breached Colonial Pipeline Using Compromised Password*. Forbes, June 4, url: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

UNCTAD (2021). Cybercrime Legistaltion Worldwide. https://unctad.org/page/cybercrime-legislation-worldwide

About the Author

Pratim Milton Datta is a professor of Cybersecurity and Digital Transformation at the Ambassador Crawford College of Business and Economics at Kent State University, USA, and a Senior Research Associate at the University of Johannesburg, South Africa. Pratim previously served as the the PhD Director and the AACSB Assurance of Learning Lead for the College. Pratim has over 50 journal publications. Prior to academia, Pratim worked in Global IT consulting.

Thomas Acton is a professor in Business Information Systems at the National University of Ireland (NUI) Galway, Ireland. From 2015 through 2020 he was Head of School of Business & Economics. Previously he was Vice Dean for Teaching & Learning, and Head of the discipline of Business Information Systems. He has served as associate editor on a number of journals, including the European Journal of Information Systems and the Journal of Theoretical and Applied E-Commerce Research. Prior to joining the university he worked in the software and private education sector.