Fresh Phish: Colonial Pipeline Ransomware Hack Unleashes Flood of Related Phishing Attempts

inky.com/blog/colonial-pipeline-ransomware-hack-unleashes-flood-of-related-phishing-attempts

Posted by Roger Kay

- Tweet
-

Among other things, phishers are avid newshounds. They read the press diligently looking for topics that might help them more successfully fool targets, land malware, and extract value. The highly visible ransomware attack recently executed by Eastern Europe-based hacker group DarkSide against Colonial Pipeline, a Houston-based oil pipeline operator, drew a lot of phisher interest, and, voila! Within a couple of weeks, new phishing attempts were unleashed on a world suddenly aware of Colonial and the exploitation of its vulnerabilities.

These new attempts tried to leverage the Colonial attack with clever pitches. INKY, the foremost anti-phishing technology on the market today, started seeing these attempted attacks almost immediately following the public humiliation of Colonial, which ended up paying $5 million to DarkSide to unlock its data.

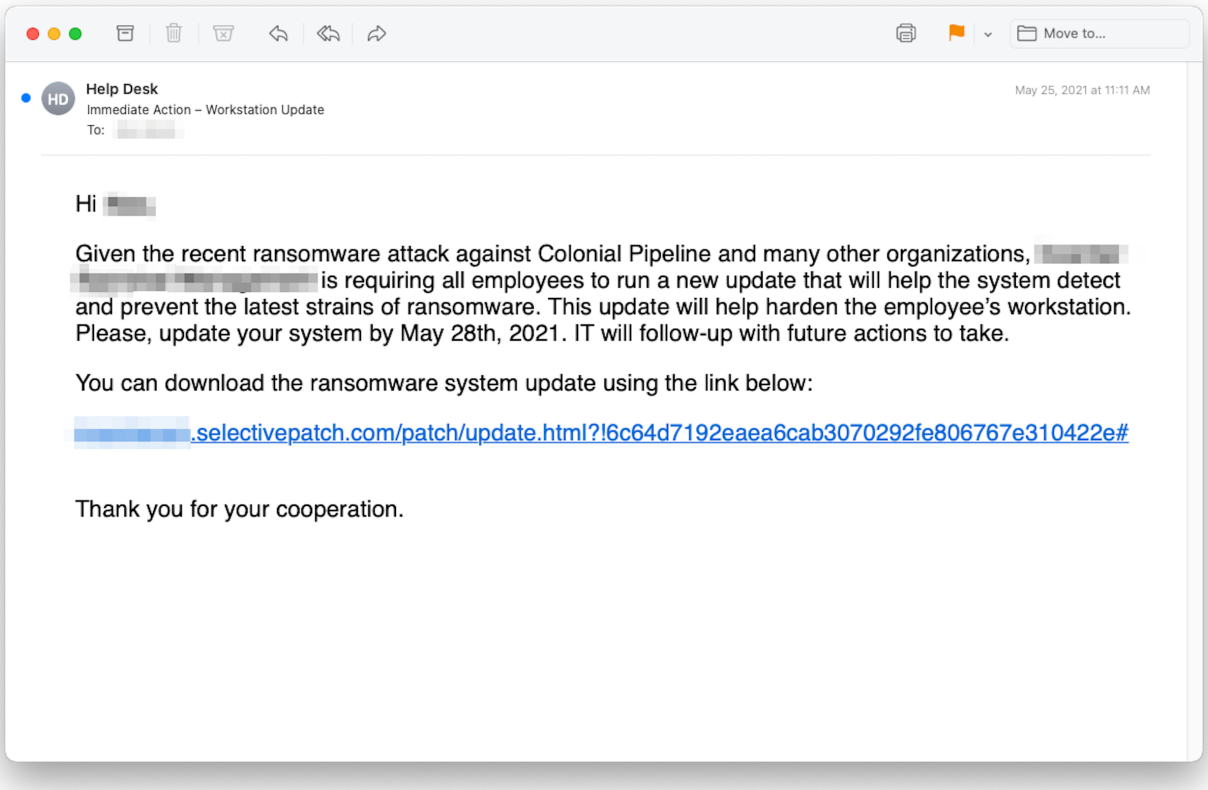
Quick Takes: Attack Flow Overview

- **Type**: phishing
- **Vector**: email, malware download from abused free site

- **Payload**: abused legitimate penetration-testing tool that launches ransomware, surveillance, or data exfiltration campaign
- **Techniques**: targeted phishing email tries to trick the recipient into downloading an "update," which is supposedly related to the Colonial Pipeline vulnerability but is really malware
- **Platform**: Office365
- **Target**: Corporate-wide surveillance, data exfiltration, ransomware shutdown

The Attack

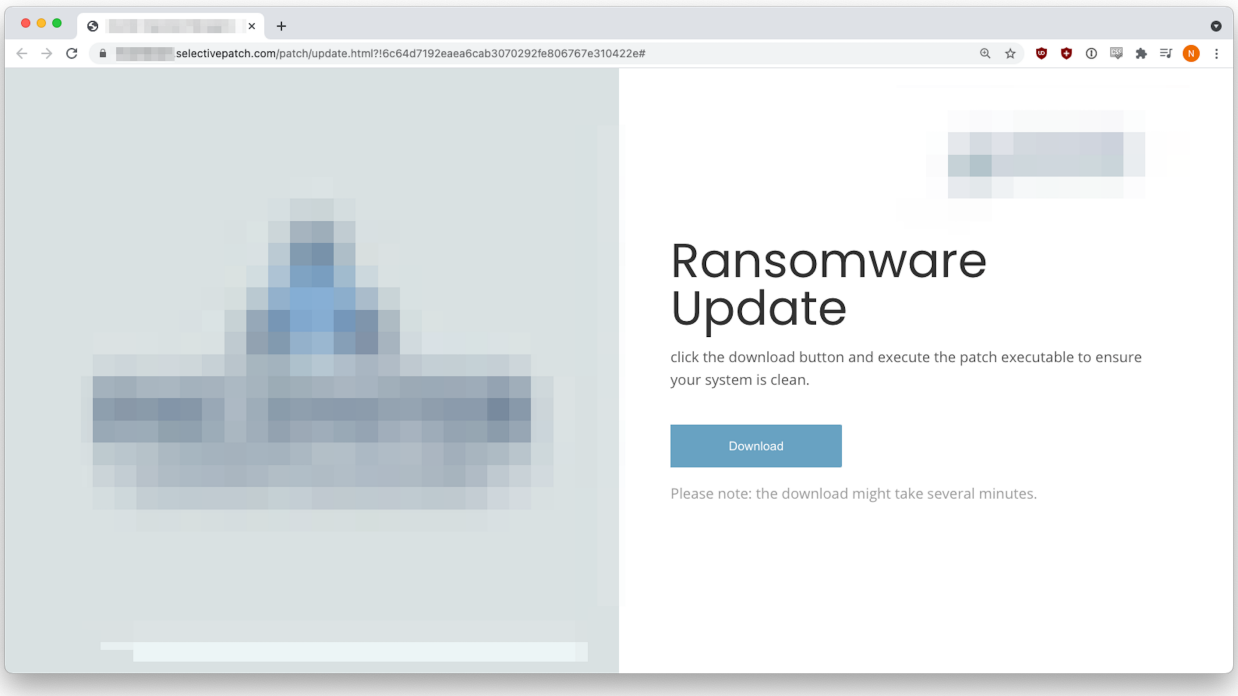
Several INKY users received "helpdesk" emails like the one below with instructions to download a "ransomware system update" from an external site.

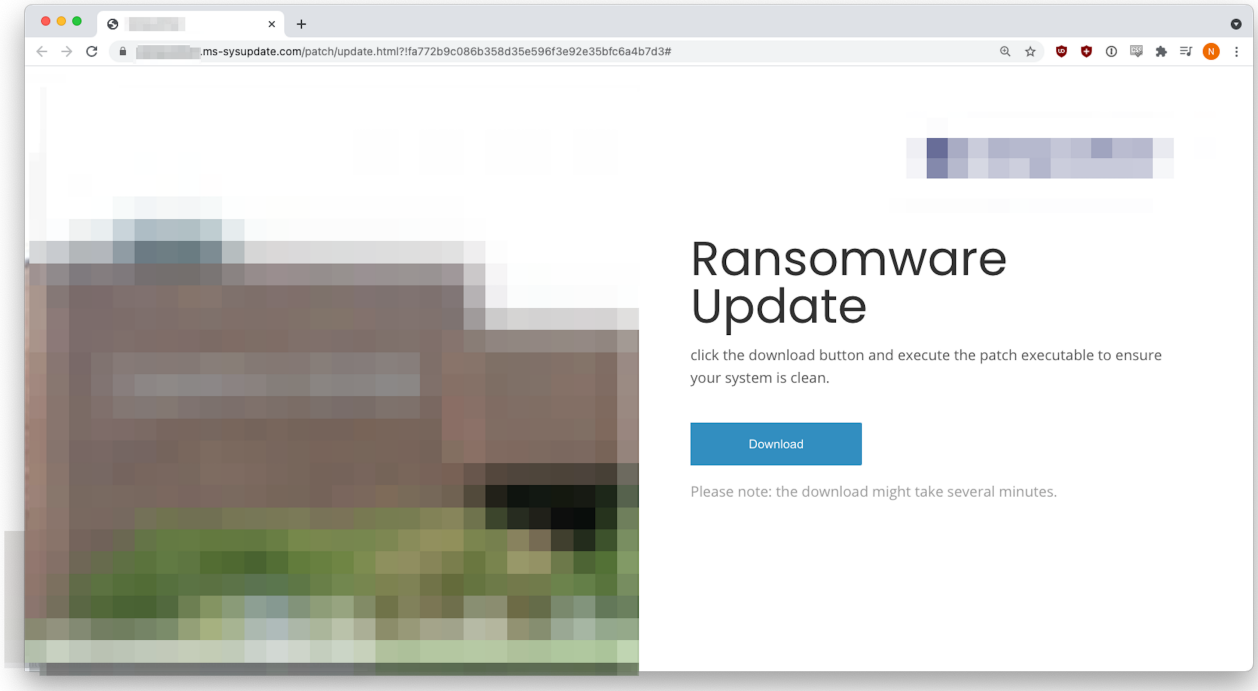


The malicious emails were sent from newly created domains (ms-sysupdate.com and selectivepatch.com) controlled by cybercriminals. The domain names, sufficiently plausible to appear legitimate, were nonetheless different enough so that garden variety anti-phishing software would not be able to use regular expression matching to detect their perfidy. INKY, of course, caught the phish using other techniques, which is why they're on display here.

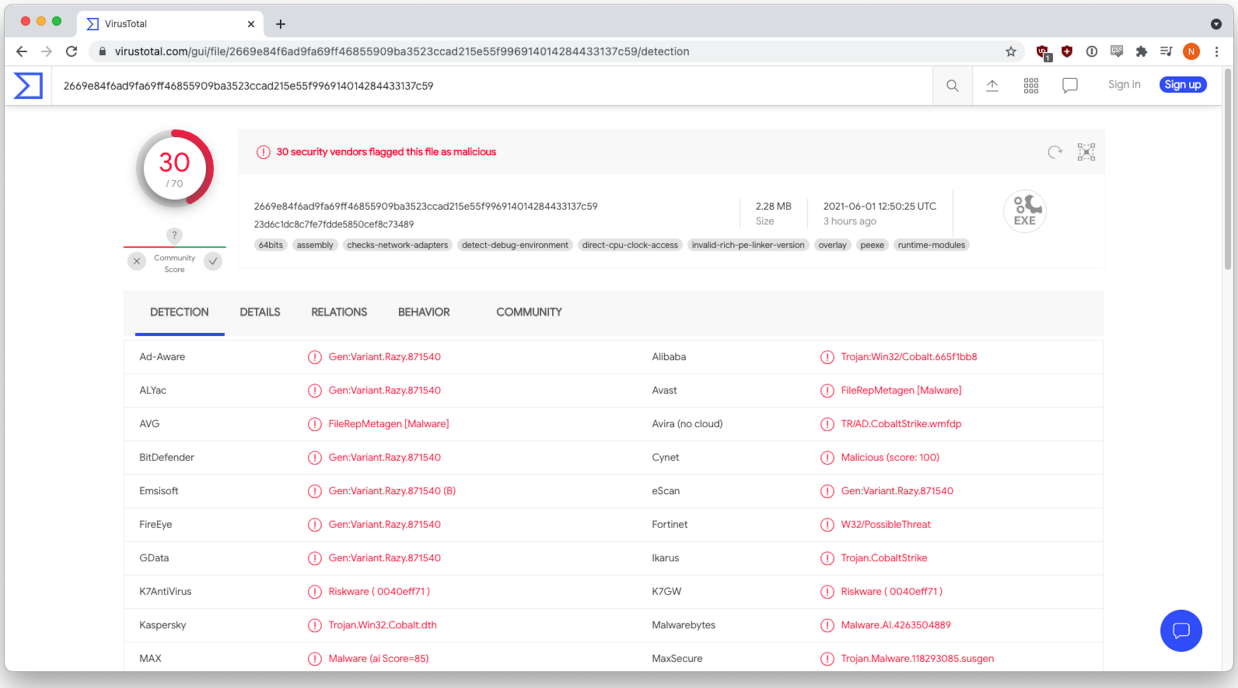
```
Domain Name: MS-SYSUPDATE.COM
Registry Domain ID: 2613602127_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2021-05-20T15:31:19Z
Creation Date: 2021-05-20T15:03:35Z
Registry Expiry Date: 2022-05-20T15:03:35Z
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
```

Both domains were registered with NameCheap, a registrar popular with bad actors. Its domains are inexpensive, and the company accepts Bitcoin as payment for hosting services (handy for those trying to remain anonymous). The malicious links in the emails belonged to — surprise! — the same domain that sent the emails. Convenient, right?





In this highly customized attack, the malicious site used the target company's logo and imagery. The innocuous "Download" button was set to download a malware file called "Ransomware_Update.exe". What could possibly go wrong?



The malware was, in fact, "Cobalt Strike," a legitimate penetration-testing tool that has been deeply abused by bad actors since its source code was leaked in late 2020. This abuse has been linked to ransomware, surveillance, and data exfiltration campaigns. According to Talos

Intelligence, 66% of ransomware attacks in 4Q20 involved “Cobalt Strike.” This serious payload is designed for maximum impact.

Techniques

Colonial-Pipeline-follow-on attacks were based on the confluence of two factors, the Colonial ransomware attack itself and the recent public availability of a highly effective remote-access tool. The Colonial Pipeline ransomware attack raised the visibility of ransomware in general. Whether they operate in infrastructure or are dependent on it (which includes practically everyone), people were primed by the news cycle to be thinking about ransomware issues. In this environment, phishers tried to exploit people’s anxiety, offering them a software update that would “fix” the problem via a highly targeted email that used design language that could plausibly be the recipient’s company’s own. All the recipient had to do was click the big blue button, and the malware would be injected.

Recap of Techniques:

- Dynamic Phish — uses elements of the target’s company’s brand elements to look legitimate if not internal
- Abused Free Website — evades URL analysis by traditional email security products
- Malware Injection — A recipient click initiates the injection of a legitimate but abused remote access tool that allows the abuser to control the target’s system
- Trusted Logo Imagery — gains the confidence of target recipient, furthering the likelihood of a successful exploit

Best Practices: Guidance and Recommendations

Phishers are getting better at camouflage. They try to make their emails look as if they come from the target’s employer, lending them an air of greater legitimacy. By using newly created domains, the email can evade traditional phishing analysis, which looks only at commonly accepted email tags DKIM and SPF and sees nothing suspicious. The important analysis to be done here is not whether the email comes from a legitimate host but whether it comes from where it appears to come. If it looks as if it was sent by the company itself (e.g., from HR, IT or Finance), does it in fact originate from an email server under the company’s control? If it looks like the HR or IT Departments but deviates from the norm, that should be a flag.

In addition to using better camouflage, phishers excel at leveraging current events and other cyber-attacks to create urgency in their communications. In this case, no doubt many recipients wanted to “do the right thing and help out the IT team” by clicking on the bad link. Attackers use these emotions to trick users into doing things they might not otherwise do. An IT policy stating that employees will not be asked to download certain file types might be a good start to combat attacks like this. A standard and formalized communications protocol that is widely shared, and frequently reinforced, would help as well.

And of course, an anti-phishing software like INKY that performs this sort of analysis, can alert recipients of inaccurate email sources and potential harm, and direct appropriate actions via a banner in the email.

———

INKY® is the most effective hero in the war against phishing. An award-winning cloud-based email security solution, INKY® prevents the most complex phishing threats from disrupting or even immobilizing your company's day-to-day business operations. Using computer vision, artificial intelligence, and machine learning, INKY® is the smartest investment you can make in the security of your organization. INKY® is a proud winner of the NYCx Cybersecurity Moonshot Challenge and finalist in the 2020 RSAC Innovation Sandbox Competition. Learn more about INKY® or request an online demonstration today.

Topics:

- Phishing,
- Fresh Phish