



AUGUST 4-5, 2021

BRIEFINGS

The Kitten that Charmed Me: The 9 Lives of a Nation State Attacker

Richard Emerson, Senior Threat Hunt Analyst
Allison Wikoff, Senior Strategic Cyber Threat Analyst
IBM Security X-Force Threat Intelligence

#BHUSA @BlackHatEvents

>whoami



Richard Emerson

Senior Threat Hunt Analyst, IBM Security X-Force
10 years experience in research, intelligence analysis, network defense
MIT Lincoln Labs, Department of Defense



Allison Wikoff

Senior Strategic Cyber Threat Analyst, IBM Security X-Force
20 years experience in research, intelligence analysis, network defense, IR
SecureWorks, Federal Reserve System, etc.

Today's Talk – ITG18

Details of ITG18 operations via opsec mistakes including:

- How do they operate?
- What tools do they use?

Our 40 Minute Goals

- What can we learn from their mistakes

Research Available

- <https://ibm.biz/ITG18Blunder2020>
- <https://ibm.biz/ITG18Blunder2021>



This is not an attribution talk

**IBM performed responsible disclosure in
the course of doing this research**

Research Genesis

Routine information gathering on ITG18 infrastructure leads to discovery of an open file directory...

Files uploaded over course of a week before taken down by threat actor

Included exfiltrated victim data and... **4+ hours of desktop recordings!**

ITG18 Open Directory File Listing









 AOL	AVI File
 Aol Contact	AVI File
 bandicam 2020-05-09 02-52-41-389	AVI File
 bandicam 2020-05-09 05-40-48-834	AVI File
 bandicam 2020-05-10 02-51-51-155	AVI File
 Gmail	AVI File
 Hotmail	AVI File
 Yahoo	AVI File

Image source: IBM Security X-Force



How we define ITG18

Objectives

- Espionage and surveillance likely in support of Iranian government objectives

Targets

- Iranian and near abroad dissidents, journalists, academics; Reformist political party members
- COVID researchers, US politicians, nuclear regulators, financial regulators

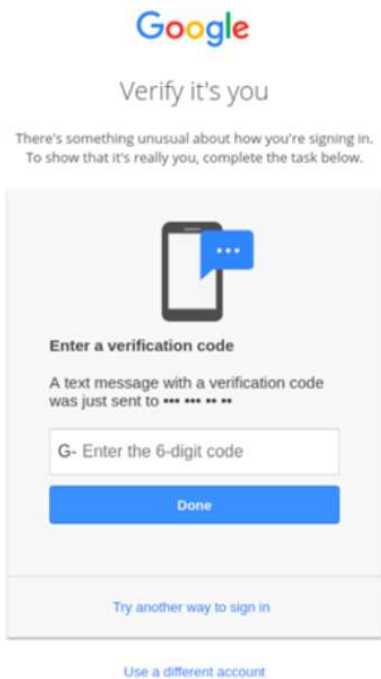
Tactics

- Phishing (email, social Media, SMS), credential harvesting, leveraging compromised accounts, masquerading as legitimate organizations/individuals

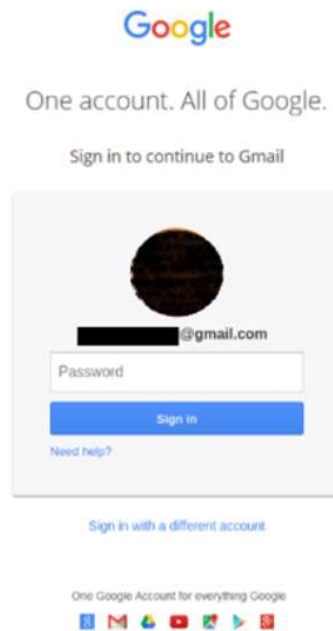
Infrastructure

- Frequently lease virtual private servers, register their own domains

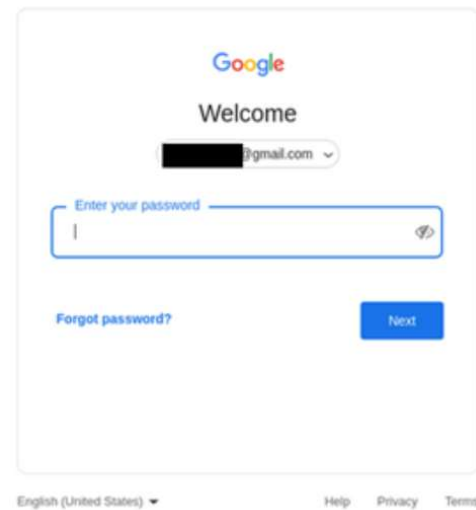
Enduring Operations



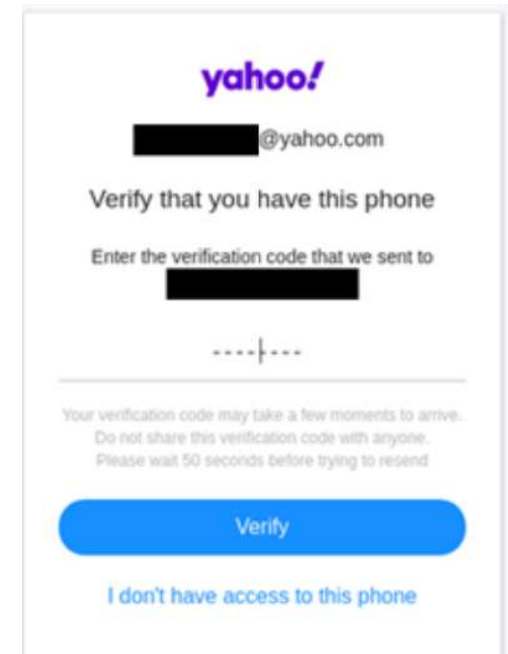
2017



2018



2019



2020

Response to Public Disclosure



COMPLAINT

Plaintiff MICROSOFT CORP. ("Microsoft") hereby complains and alleges that JOHN DOES 1-2 (collectively "Defendants"), have established an Internet-based cyber-theft operation referred to as "Phosphorus." Through Phosphorus, Defendants are engaged in breaking into the Microsoft accounts and computer networks of Microsoft's customers and stealing highly sensitive information. To manage and direct Phosphorus, Defendants

March 2019 Criminal complaint against ITG18

Source: Microsoft

- March 2019 – Microsoft wins criminal complaint to sinkhole 99 ITG18 domains

- Example domain sinkholed March 27, 2019:

identifier-services-sessions . info

- ITG18 response to domain take down three weeks later:

identifier-services-sessions sitfo

Historical Tools

Metasploit – Commercially available pentesting framework

Spynote – Commercially available Android RAT (cracked versions available)

AndroRAT – Open-source Android RAT (similar to: <https://github.com/karma9874/AndroRAT>)

pdfReader – Custom modular Windows backdoor

pdfReader Modules

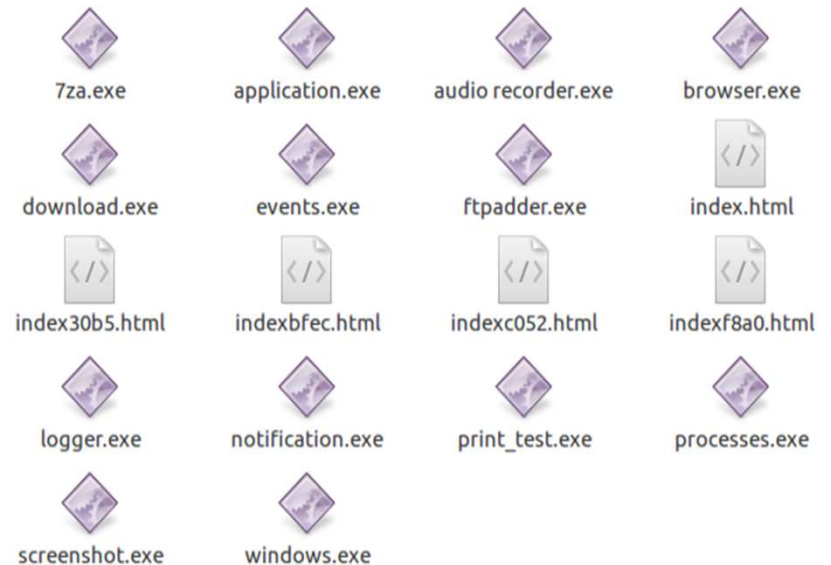
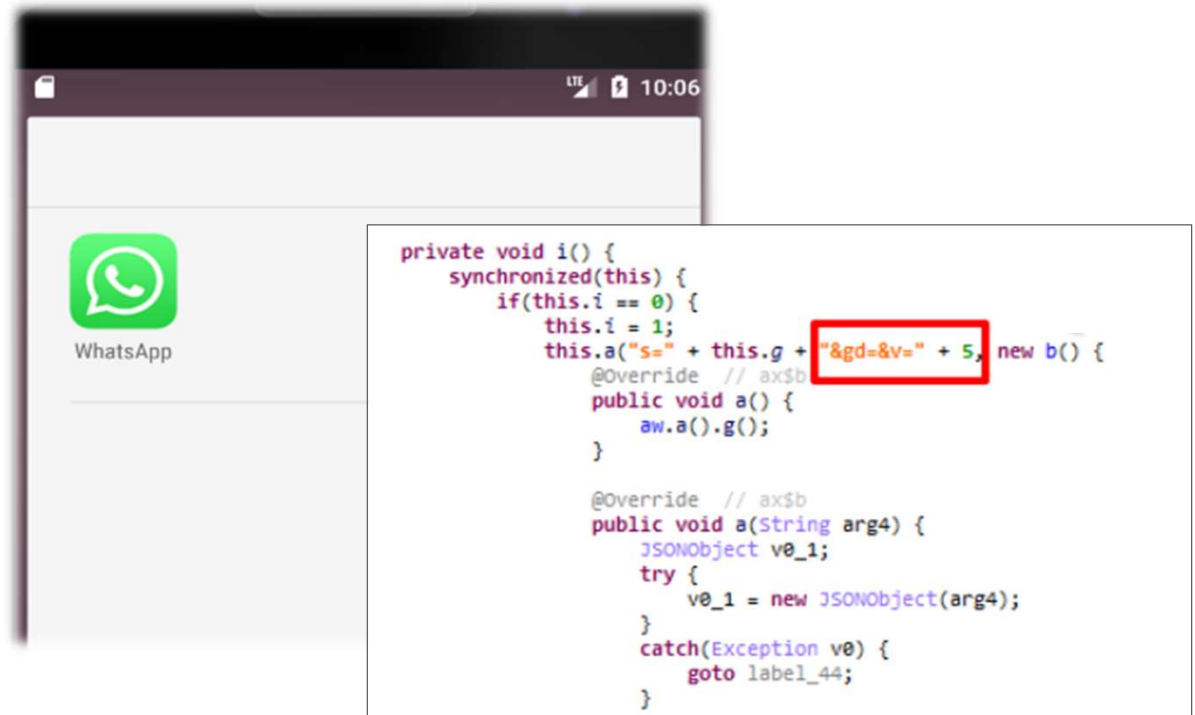


Image Source: IBM Security X-Force

LittleLooter

- Masquerades as WhatsApp for Android
- Multi-functional backdoor
- HTTP/SMS C2 communications

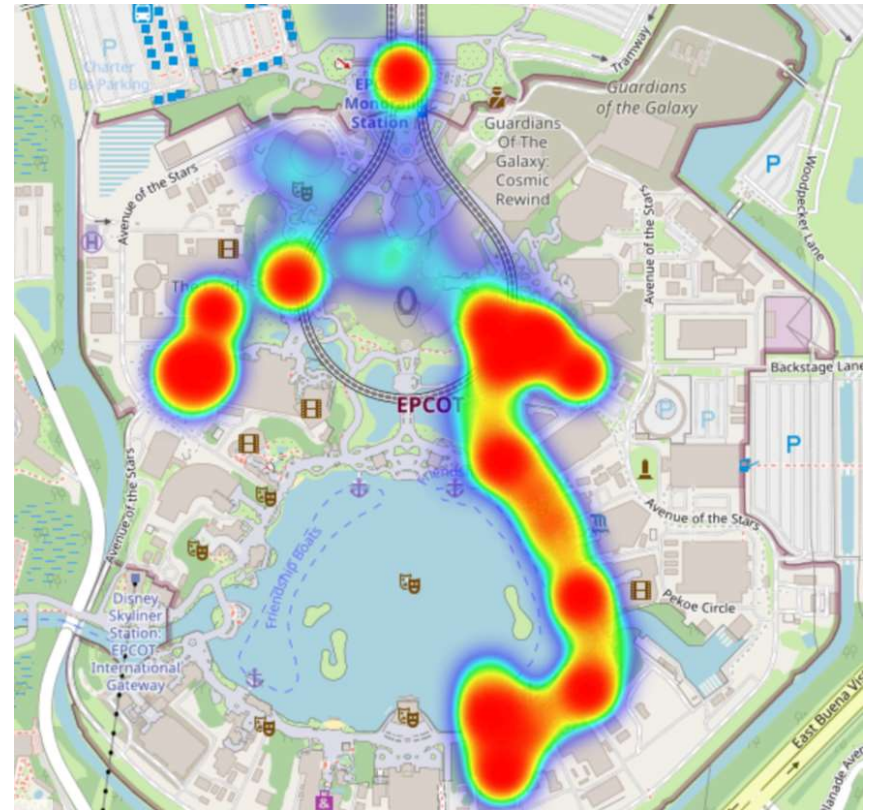
- Sample discovered by X-Force in October 2020, uploaded to VirusTotal December 2020
- Has hardcoded version number "5"
- More details available <https://ibm.biz/ITG18Blunder2021>



Images source: IBM Security X-Force

ITG18 Operational Overview

- Exfiltrated at least 2 Terabytes since Fall 2018
- Personal information
 - Location Details
 - Audio
 - Video
 - Photos
 - Chat logs and SMS messages
 - Search history
- Social media and email accounts compromised
- Some data taken via legitimate account tools



Exfiltrated data from an ITG18 victim. Image source: IBM Security X-Force | Location History Visualizer

Other Historical Mistakes – Naming Your Targets

```
<title>Targets</title>
```



ITG18 Open Server. Image source: Shodan

Other Historical Mistakes – Copying your C2 Directory

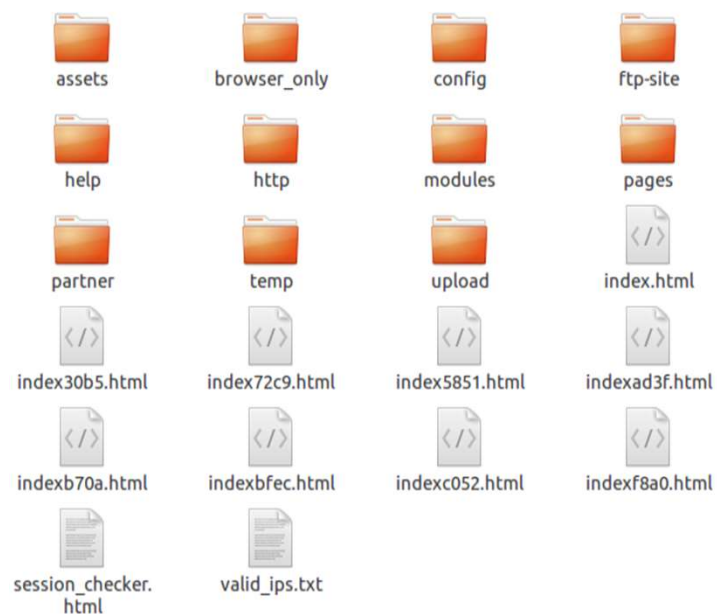


Image source: IBM Security X-Force

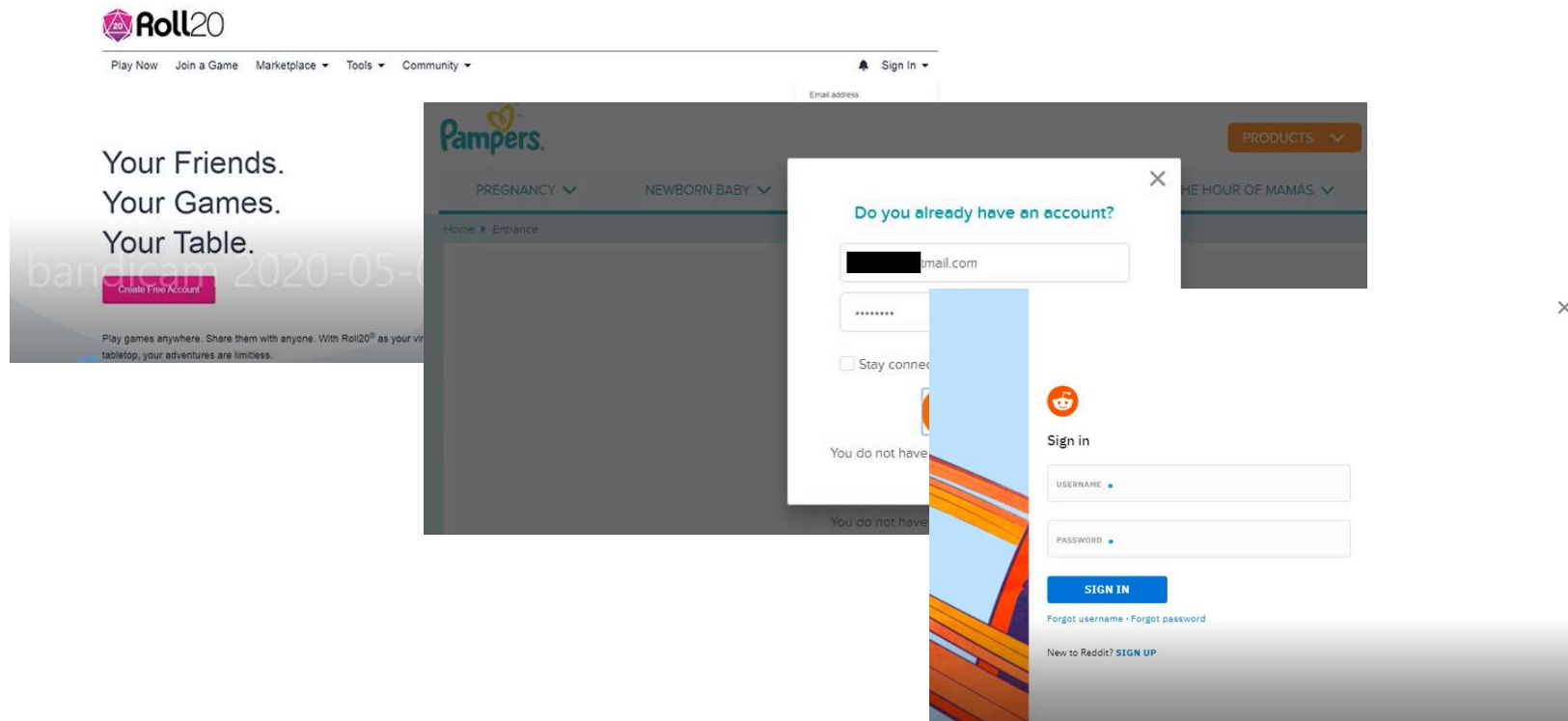
Other Historical Mistakes – Not Updating Server Software

apache_pb.gif.SATANA	2019-05-03 09:08 3.2K
apache_pb.png.SATANA	2019-05-03 09:08 2.3K
apache_pb2.gif.SATANA	2019-05-03 09:08 3.3K
apache_pb2.png.SATANA	2019-05-03 09:08 2.4K
apache_pb2_ani.gif.S.>	2019-05-03 09:08 3.0K
applications.html.SA.>	2019-05-03 09:08 2.3K
bitnami.css.SATANA	2019-05-03 09:08 3.0K
dashboard/	2019-05-03 09:08 -
favicon.ico.SATANA	2019-05-03 09:08 8.5K
forbidden/	2019-05-03 09:08 -
how_to_back_files.html	2019-05-03 09:08 4.7K
img/	2019-05-03 09:08 -
index.html.SATANA	2019-05-03 09:08 1.2K
index.php.SATANA	2019-05-03 09:08 1.2K
restricted/	2019-05-03 09:08 -
tmp/	2019-05-03 09:08 -

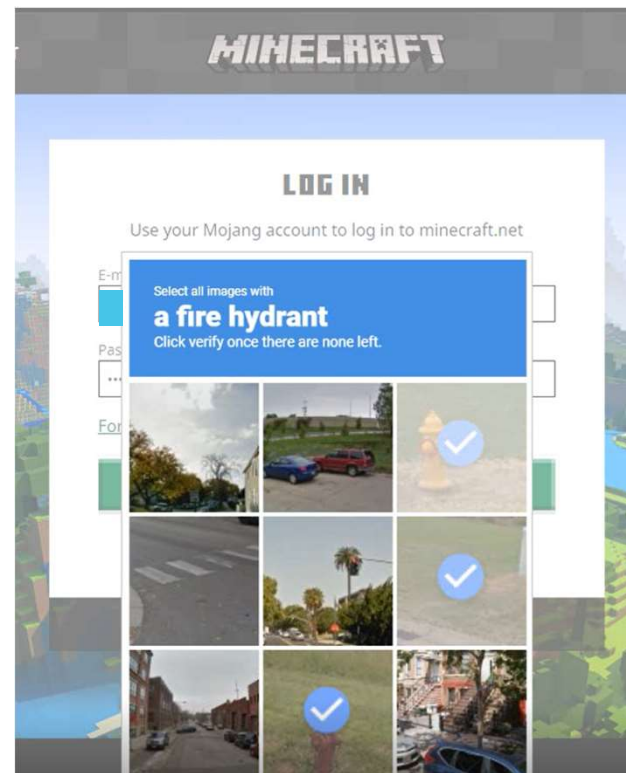
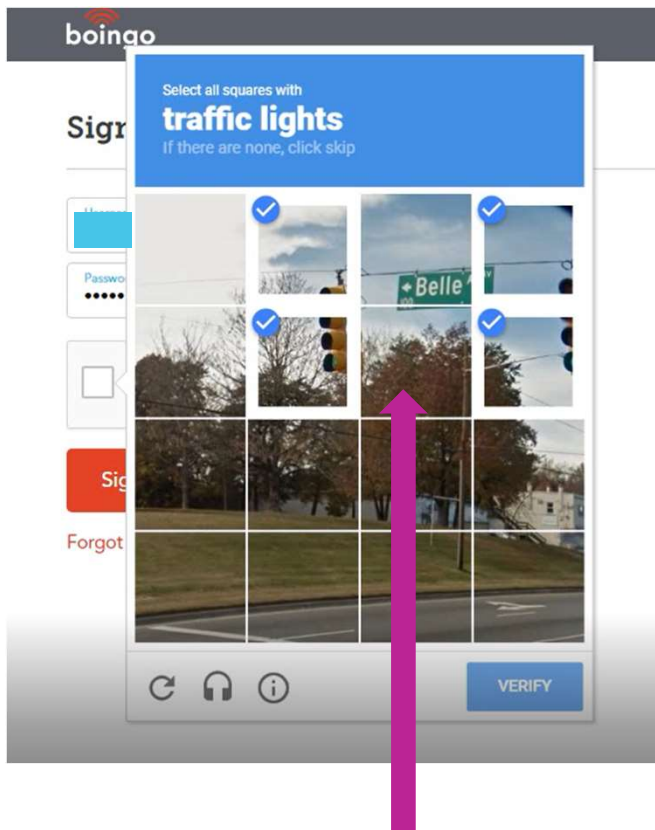
← Possible GlobelImposter ransom note

Image source: Shodan

Size of Operations – Manual Credential Validation



Size of Operations – CAPTCHA Challenges



Images source: IBM Security X-Force

Size of Operations – Individual Operator Boxes?

Name	Last modified	Size	Description
+98...rar	2020-08-23 01:53	12G	
+98...rar	2020-08-23 02:21	4.6G	
+98...rar	2020-08-23 02:24	6.7G	
+98...rar	2020-08-23 02:07	1.0G	
+98...rar	2020-06-27 22:36	76M	
+98...rar	2020-10-05 23:27	205M	
1.rar	2020-08-11 08:28	128G	
94.110.rar	2020-10-21 23:50	6.7G	
94.111.rar	2020-10-22 00:27	25G	
3136.rar	2020-09-29 01:24	8.9G	
WhatsAppSetup.exe	2020-08-31 11:55	107M	
vebExpor...	2020-08-20 00:27	16G	

Valid copy of WhatsApp installer

Name	Last modified	Size	Description
+98...rar	2020-10-09 21:41	4.8G	
7.rar	2020-08-15 04:21	28G	
8728.rar	2020-09-23 23:56	2.6G	
New Text Document.txt	2020-09-10 07:03	0	
WhatsApp.apk	2020-08-24 00:00	8.1K	
WinRAR.5.90/	2020-05-30 09:58	-	
programs.rar	2020-05-30 09:46	1.1G	
...ra	2020-08-19 05:14	797M	
session1.rar	2020-08-10 19:21	238M	

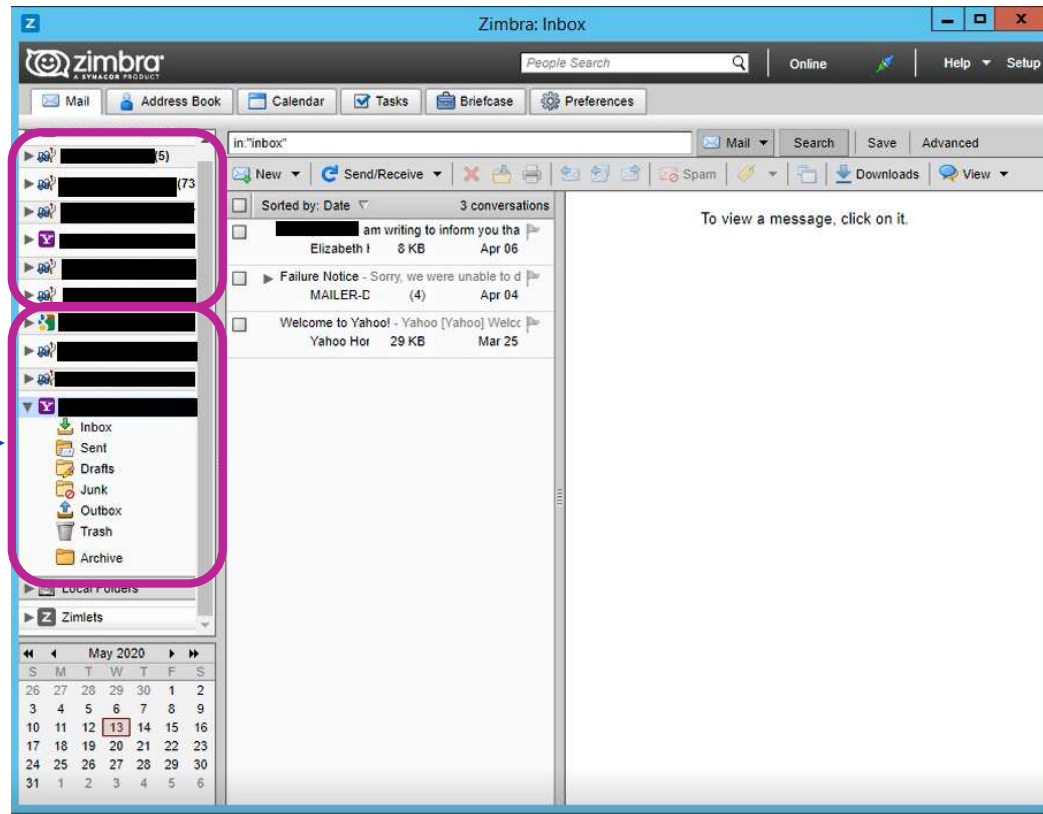
LittleLooter
Android
malware

Size of Operations – Individual Operator Boxes?

Compromised accounts



Operator accounts



Size of Operations - Summary

- ~ 2000 unique indicators
- ~ 2 Terabytes of victim exfil
- Manual data exfiltration, credential validation
- 10 - 20 intermediate VPN servers active at any time
- Blended strategic objectives
- Broad and targeted phishing operations
- Long running operation
- Loads of repeat mistakes
- **Training videos**



Image source: *Office Space*. Dir. Mike Judge. Twentieth Century Fox, 1999.


“Training Videos” – A Primer

- Discovered on an open server that previously hosted ITG18 infrastructure
- Desktop recordings made by the operator using free screen recording software
- Persona accounts on AOL, Yahoo, Gmail and Hotmail
- Operator demos setting up account for continuous monitoring using an email collaboration platform
- Operator demos exfiltrating information on various web mail platforms

We have blurred out identifying victim and persona information in the videos



Image source: IBM Security X-Force

The image features a dark teal background with a glowing, wavy, particle-based pattern at the top. The pattern consists of numerous small, light-colored dots that form a series of undulating lines, creating a sense of movement and depth. The overall aesthetic is modern and digital.

Thank you!