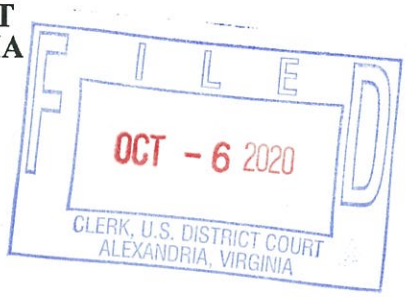
IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division



MICROSOFT CORPORATION, a Washington corporation, and FS-ISAC, INC., a Delaware corporation,

Plaintiffs,

v.

JOHN DOES 1-2, CONTROLLING A COMPUTER BOTNET AND THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS,

Defendants.

Civil Action No: 1:20cv1171

FILED UNDER SEAL

DECLARATION OF KEVIN GARLOW IN SUPPORT OF PLAINTIFFS' APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Kevin Garlow, declare as follows:

1. I am a Lead Information Security Engineer at Lumen Technologies ("LUMEN"), formerly known as CenturyLink. LUMEN is a global technology company, which provides a wide variety of telecommunications and technology products and services. Included in these offerings, LUMEN provides security services across the world and operates a team focused on identifying, understanding, and preventing Internet-based threats. As a member of that team, I make this declaration in support of Plaintiffs' Application For An Emergency Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge, and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein, via telephone or remote video session.

2. I have worked in the information technology field for 26 years, in areas such as

database administration, system administration, and cybersecurity. In my current role at LUMEN, I identify Internet-based threats and track them over time. Through this work, I have expertise in using network data to identify potential threats and use my knowledge and the tools developed by my team to confirm those threats. Prior to joining this team, I was focused on a variety of other software technologies and their operation at LUMEN. My expertise in cybersecurity comes from work experience, self-driven learning, and a foundation built through studying Astrophysics and Computer Science at Villanova University. I continue to enhance my learning and knowledge about security matters and share information with members of the security industry focused on tracking botnets. Attached hereto as **Exhibit 1** is a true and correct copy of my resume.

3. Through LUMEN's reverse-engineering of the malicious software Trickbot, we were able to extract the unique communication protocols and encryption techniques utilized by the software. These findings were used to build an application which can validate computers operating as controllers of the Trickbot botnet. This technique has been used by LUMEN to identify and remove thousands of botnet controllers for other malware families since 2017, and we began applying the technique to the Trickbot botnet within the last year.

4. During our investigation, LUMEN has used the validator technology to positively identify 502 unique IP addresses acting as controllers of the Trickbot botnet. Our identification comes from monitoring the behavior of this threat in our network, extracting possible new botnet controllers, and then validating they communicate in the specific nature of the Trickbot malware family with the previously mentioned application. Of all botnet controllers identified by LUMEN during this time period, Trickbot accounted for 13%.

5. During our investigation, LUMEN has sent notifications to Internet Service

Providers (ISPs) and server hosting providers, alerting them of the presence of Trickbot controllers on their networks and seeking to get them removed. These notifications were sent to at least 131 distinct email addresses designated for reporting abuse.

6. Despite LUMEN's attempts to have the Trickbot controllers removed through the normal procedure of reporting abuse to providers, there are over 40 Trickbot controllers which remained online after more than 30 abuse notifications. 9 Trickbot controllers remained online after more than 100 such notifications. In addition, we identify new Trickbot controllers coming online every month. We confirmed 55 new Trickbot controller IPs in September 2020, and 99 new Trickbot controller IPs in August.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed this 4th day of October, 2020, in Denver, Colorado.

Kevin R. Garlow

EXHIBIT 1

KEVIN GARLOW

Summary

Kevin Garlow is a seasoned information technology professional with a special interest in cybersecurity. He currently researches and analyzes malicious threat actors on the Internet: botnets, crimeware, and advanced persistent threats (APTs). In the past he has performed diverse roles such as system administrator, developer, database administrator, web server administrator, and consultant, on a variety of applications, platforms, and operating systems. He also regularly acts as a technical leader, mentoring peers to increase their knowledge and abilities.

Education

- College courses in cybersecurity (based on CISSP certification domains), **Regis University, Denver, CO**
- Completed course work toward a Ph.D. in Planetary Sciences, **University of Arizona, Tucson**
- B.S. in Astronomy and Astrophysics, Minor in Computer Science, **Villanova University, Pennsylvania** (Graduated Magna Cum Laude, Phi Beta Kappa)

Certifications

- Oracle Certified Professional Database Administrator (OCP DBA) on Oracle version 11g
- Previously certified Oracle Database Administrator on Oracle versions 7, 8, 8i, and 9i

Employment History

Lumen (formerly CenturyLink, formerly Level 3, formerly tw telecom) – ***from 2010 to present***

Positions held:
Lead Information Security Engineer – 2019 to present
Lead IT Systems Analyst – 2018 to 2019
System Administrator – 2015 to 2018
ERP Systems Administrator – 2010 to 2015

- Analyzed netflow and DNS data for suspicious IPs and domains
- Created and maintained JupyterLab notebooks and shell scripts to automate extracting, summarizing, and sharing data about botnets and controllers with research partners
- Investigated presence of VPN devices on our network vulnerable to newly-released exploits, and coordinated notification and remediation
- Wrote code in Python to create data visualizations
- Wrote code in Python and JupyterLab notebooks to extract and analyze data from Big Data cluster running Hadoop and YARN
- Designed, coded, tested, and tuned software programs to reliably convert data between disparate systems, using PL/SQL and shell scripts, as part of large application re-implementation
- Managed batch execution and data ETL systems such as UC4/Automic, Lavastorm, and Data3Sixty Analyze
- Wrote multiple interface programs using SQR and batch scripts for encrypting and sending data to and from partners

- Designed architecture; specified, installed and configured servers for external-facing B2B Supplier Portal, including all layers of the required infrastructure
- Selected, installed, and configured host-based antivirus for B2B Supplier Portal
- Helped ensure production systems were protected against several major security vulnerabilities which emerged in 2014 (HeartBleed, Shellshock, and POODLE).
- Managed and performed technical upgrades of PeopleSoft ERP applications (HR, Financials)
- Configured and managed multiple servers and virtual machines (web server, app server, batch server, load balancer) for ERP applications
- Performed troubleshooting and tuned performance of databases and applications

Lifesaver Consulting – ***from 2006 to 2010***
Principal Consultant

- Performed technical upgrades of PeopleSoft ERP (HR, Financials, CRM) systems for a variety of clients, on Oracle and SQL Server databases
- Deployed PeopleSoft Talent Acquisition Manager (HR) over internet. Obtained SSL certificate, enabled SSL/https, and modified PeopleSoft-delivered Javascript to enforce custom security requirements

Nakoma Group (Denver, CO) – ***from 2004 to 2006***
Technology & Upgrade Lab Manager / DBA / System Administrator / PeopleSoft Administrator

- Planned and managed resources, scheduling, and deliverables for multiple simultaneous client projects
- Performed database administration on multiple platforms (Oracle, SQL Server, Informix, DB2)
- Administered, maintained, upgraded and monitored Unix and Windows servers in support of Technology and Upgrade Lab
- Wrote scripts to monitor and report on disk space utilization, server availability, and service availability
- Maintained secure firewall throughout to secure appropriate use by consultants and clients
- Migrated all lab servers and systems to new hardware running Windows 2003 and Linux
- Installed and configured Red Hat Enterprise Linux server to replace an aging Compaq Tru64 server
- Installed Oracle 9i and migrated 9 live databases to the new server
- Performed all necessary network and firewall changes to deploy servers to a co-location facility
- Configured and administered virtual machines running under Virtual Server 2005 R2

The Implementation Partners (Denver, CO) – ***from 2000 to 2003***
Senior Applications Specialist

- Performed technical upgrades of PeopleSoft ERP systems for a variety of clients, on Oracle, Informix, and DB2 databases
- Improved application and database performance for a variety of clients (Oracle, DB2, Microsoft SQL Server)

British Home Stores [BHS] (London, UK) – ***from 1998 to 1999***
Independent PeopleSoft Oracle DBA

- PeopleSoft DBA – Fin 7 implementation (GL, AP, PO, AM, IN, AR) – Oracle

Cambridge Technology Partners (Cambridge, MA) – ***from 1997 to 1998***
Senior Applications Specialist

- Implemented and upgraded PeopleSoft ERP systems for a variety of clients, on Oracle and DV2/MVS databases
- Improved application and database performance for a variety of clients (Oracle, DB2, Microsoft SQL Server)

El Paso Water Utility (El Paso, TX) – ***from 1995 to 1997***
Independent PeopleSoft Oracle DBA

- PeopleSoft Oracle DBA, Unix SysAdmin, Technical Lead – Implementation and upgrade of HR (4.0 to 5.0); Implementation and upgrade of Public Sector Financials (3.0 to 5.0) – Oracle 7

Avalon Software (Tucson, AZ) – ***from 1994 to 1995***
Senior Architecture Engineer

- Database programming and administration (Oracle 6 and 7), software development, system administration