**IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

MICROSOFT CORPORATION **Plaintiffs,** **v.** **JOHN DOES 1-51, CONTROLLING MULTIPLE COMPUTER BOTNETS THEREBY INJURING MICROSOFT AND ITS CUSTOMERS** **Defendants.**	**CASE NO.** 1:17-CV-4566 **FILED UNDER SEAL**

DECLARATION OF VISHANT PATEL IN SUPPORT OF MICROSOFT'S APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE: PRELIMINARY INJUNCTION

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MICROSOFT CORPORATION

Plaintiffs,

v.

JOHN DOES 1-51,
CONTROLLING MULTIPLE
COMPUTER BOTNETS
THEREBY INJURING
MICROSOFT AND ITS
CUSTOMERS

Defendants.

CASE NO.

1:17-CV-4566

FILED UNDER SEAL

DECLARATION OF VISHANT PATEL IN SUPPORT OF MICROSOFT'S APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE: PRELIMINARY INJUNCTION

I, Vishant Patel, declare as follows:

1. I am a Senior Manager of Investigations in the Digital Crimes Unit of Microsoft Corporation's Legal and Corporate Affairs group. I make this declaration in support of Microsoft's Application For An Emergency *Ex Parte* 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 discussed in this declaration.

I. Introduction

2. In my role at Microsoft, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and the customers that rely on such business. As part of my day to day activity I work directly with other Microsoft subject matter experts and malware researchers to identify, investigate, and neutralize threats to Microsoft and its customers. I also participate in the investigation of botnets and participate in court-authorized countermeasures to disrupt them and to remediate their harmful effects. I have personally investigated and assisted in the court-authorized disruption or takedown of several botnets while at Microsoft, including the botnets known as Citadel and Shylock.

3. Prior to my current role, I worked as a Senior Investigator for Citigroup Inc., responding and investigating phishing attacks, malware, and system and network incidents. A copy of my curriculum vitae is attached to this declaration as **Exhibit 1**.

4. I am a member of a team of investigators actively investigating a family of botnets associated with the Gamarue malware (also known as "Andromeda" or "Wauchos" malware). Through these and related investigative steps, I have

developed detailed information about the size, scope, and illegal activities of the Gamarue botnets. In this declaration, I will explain the nature of our investigation into the Gamarue malware, as well as the proposed plan to disrupt Gamarue and significantly curtail the criminal activities that are perpetrated by Gamarue malware.

II. Microsoft's Investigation into Gamarue

5. Microsoft first detected the Gamarue malware in 2011 and subsequently identified it as one of the top malware threats to its consumers. Malware is malicious software that infects computers without the user's knowledge or consent. Since 2011, Gamarue has spread prolifically around the world. As many as three to four million computers have been infected each month with the Gamarue malware. Over 250 countries and territories have been affected by Gamarue, and at least 464 independent Gamarue derived botnets are in operation globally. Gamarue has one of the highest encounter rates of any malware that Microsoft monitors. In the maps shown in **Figure 1** and **Figure 2**, below, the red dots are associated with computers of victims that have encountered Gamarue in the United States and more specifically, the state of Georgia. **Figure 1** shows encounters across the United States totaling 3,406 from July 2016 through September 2017. **Figure 2** shows Gamarue encounters in Georgia, which occur predominantly in the Atlanta area. The encounters in Georgia total 701 from July 2016 through September 2017.

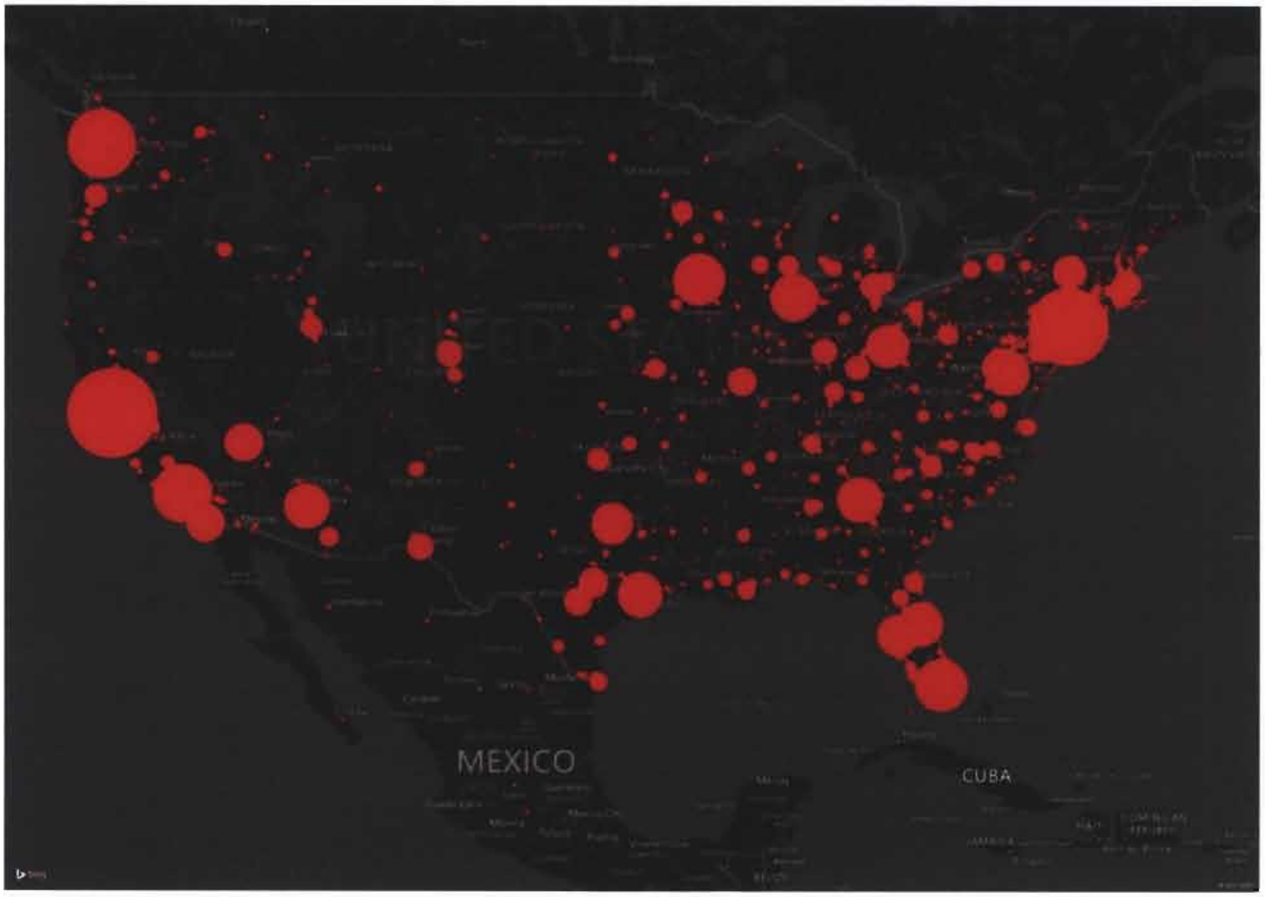

Fig. 1

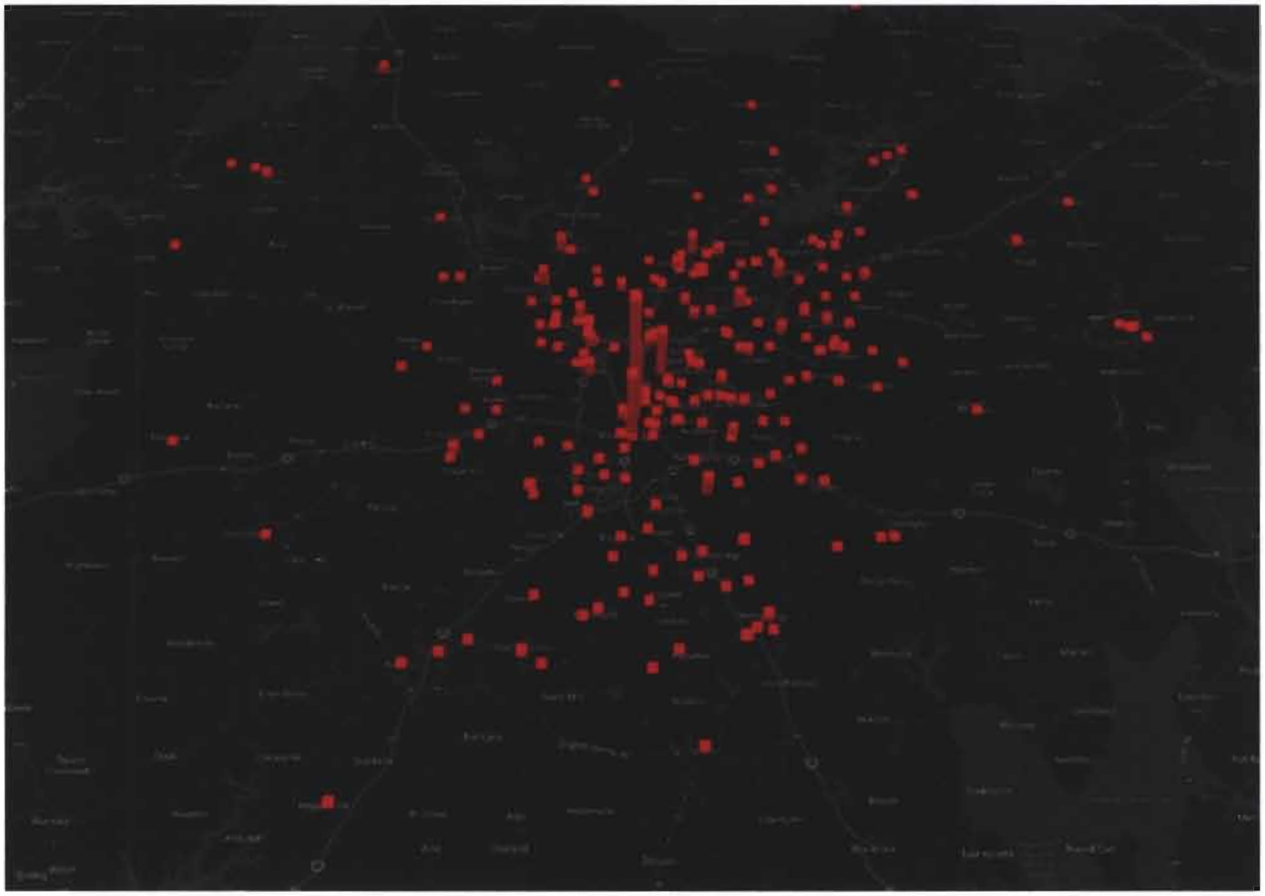

Fig. 2

6. Through my work, I am aware that Microsoft software products and solutions currently comprise approximately 35% of the total antivirus software market. When malware is encountered, the antivirus software sends data back to Microsoft, which is collected and analyzed. From this information, Microsoft has been able to determine that a significant number of malware encounters involved Gamarue.

7. In the course of Microsoft's investigation, we analyzed approximately 44,437 samples of Gamarue malware. In some cases, we purposely infected several

investigator-controlled computers with the Gamarue malware. This placed the computers under the control of the cybercriminals operating the botnet, but allowed Microsoft to analyze all of the illicit communications going to and coming from the infected computers, as well as to analyze the activities of the infected computers.

8. We observed the infected computers connect to and receive instructions from the Gamarue malware's "command and control" servers ("C2 servers"), and through this method, we believe that we identified by domain name and IP address all of the C2 servers used to control the Gamarue malware.

9. We also carefully analyzed the changes Gamarue malware makes to Microsoft's operating system and application software during the infection process, and reverse-engineered the Gamarue malware to determine its methods of operation.

III. Gamarue Command and Control Infrastructure

10. When a computer is infected with the Gamarue malware, it becomes part of a "botnet." Gamarue uses a two-tier botnet infrastructure that includes (1) an "infection tier" of infected personal computers owned by innocent and unsuspecting people, and (2) a C2 server tier used by Operator Defendants to control the computers in the infection tier. Once a computer is infected with the Gamarue malware, the malware will instruct the infected computer to contact the botnet

controller's C2 server, thus enabling Operator Defendants to control the infected computer.

11. C2 servers reside at locations on the Internet referred to as domains. Each resource on the web, such as a website like cnn.com, can be accessed through a unique domain. This domain is often presented as a user friendly name like "cnn.com," while it actually corresponds to a unique alpha-numeric value or IP address, such as 157.166.226.26.

12. The IP address can be thought of as the physical location on the Internet that corresponds to a particular domain name. C2 servers for the Gamarue malware have resided at at least 1,214 domains[1] that the Operator Defendants use to address and exchange information with the C2 servers.

13. To create an active domain, Operator Defendants must register the domain with any one of the many domain name registrars in the world. During the registration process, Defendants must associate the domain with one or more specific IP addresses.

14. Registrars obtain domain rights for their customers, such as the Operator Defendants, from registry services, which are responsible for managing

[1] Not all 1,214 domains are currently active.

domains. This includes facilitating the association between domain names and IP addresses.

15. The registry service associates a domain registered by an entity with a name server. Either the registrar or the entity that registered the domain use the name server to publish the IP address for the domain. Currently, the six domains listed in **Appendix A** to the Complaint are used in connection with the Gamarue C2 servers, and these six domains are managed by the registry services also set forth in **Appendix A** to the Complaint; a true and correct copy of **Appendix A** is attached to this declaration as **Exhibit 2**.

16. In addition to these six domains, the Defendants have used 532 domains in the past but allowed the registrations for these domains to lapse; because the now-unregistered domains could be used as backup command and control domains, these 532 domains will be registered by Microsoft concurrently with the execution of the [Proposed] Order requested by Microsoft in its Emergency *Ex Parte* Application for a Temporary Restraining Order.[2]

17. The domains used for the Gamarue malware C2 servers are hardcoded or fixed into the Gamarue source code. Once infected a computer seeks to contact

[2] In addition, 190 domains used by the Defendants have been turned into "sinkholes" by security researchers who have been involved in Microsoft's investigations of the Gamarue malware and its operation.

its C2 server, in doing so it relies on a network of servers that perform the role of keeping track of the IP address associated with every domain name on the Internet. These computers are known as Domain Name Service servers, or "DNS servers." In other words, if a person wants to connect to a website of a certain name, that person's computer needs to request the IP address of that domain from a DNS computer. **Figure 3**, below, illustrates how a computers infected with the Gamarue malware undergoes this process to navigate to a Gamarue C2 server.

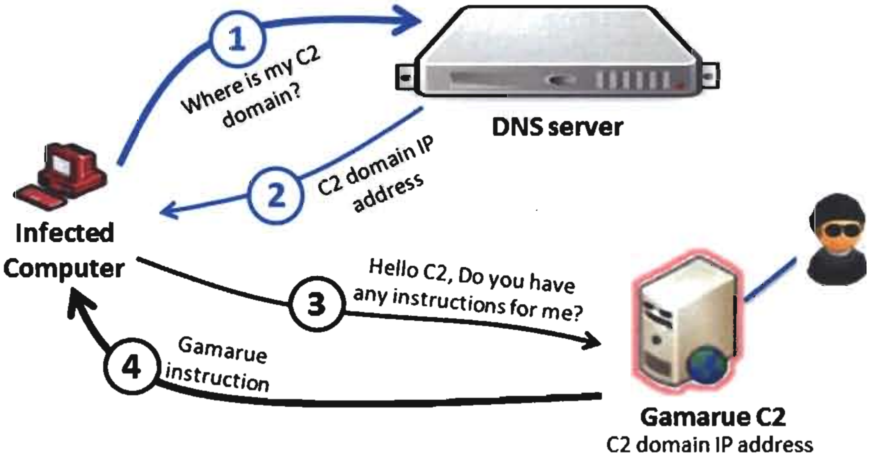

Fig. 3

18. As shown in step 1 of **Figure 3**, above, an infected computer contacts a DNS server and requests the IP address that corresponds to the C2 domain that has been programmed or hard coded into the Gamarue source code malware.

19. In step 2 of **Figure 3**, above, the DNS server facilitates delivery of the IP address that corresponds to the C2 domain.

20. The returned IP address enables the infected computer to contact the Gamarue C2 server in step 3 of **Figure 3**, above. Once the infected computer is in communication with the C2 server, Defendants can directly communicate with, and exercise control over, the infected computer.

21. In step 4, above, the communication channel enables Defendants to distribute instructions and malware to the infected computer, as well as to receive information that is uploaded by the infected computer to the C2 servers. Gamarue malware cannot connect with the C2 servers without the domains that are associated with these C2 servers.

IV. Disrupting Gamarue

22. Microsoft seeks to have the Court issue a temporary restraining order and subsequent preliminary injunction that requires the registry services listed in **Exhibit 2** to this declaration (and **Appendix A** to the Complaint) to work with Microsoft to put network infrastructure in place to route victim computer communications intended for the Gamarue domains to a Microsoft-controlled safe server, instead of the C2 servers of the Gamarue malware. This will sever ties between the Gamarue C2 servers and victim computers and allow Microsoft to take

steps that enable the owners of the infected victim computers to remove the Gamarue malware.[3]

23. This is accomplished by having the DNS servers recognize the IP address of Microsoft's safe server as the IP address for the Gamarue C2 domains. The resulting communication flow is illustrated in **Figure 4**, below. A comparison of **Figure 3** and **Figure 4** demonstrates the effects of Microsoft's requested relief.

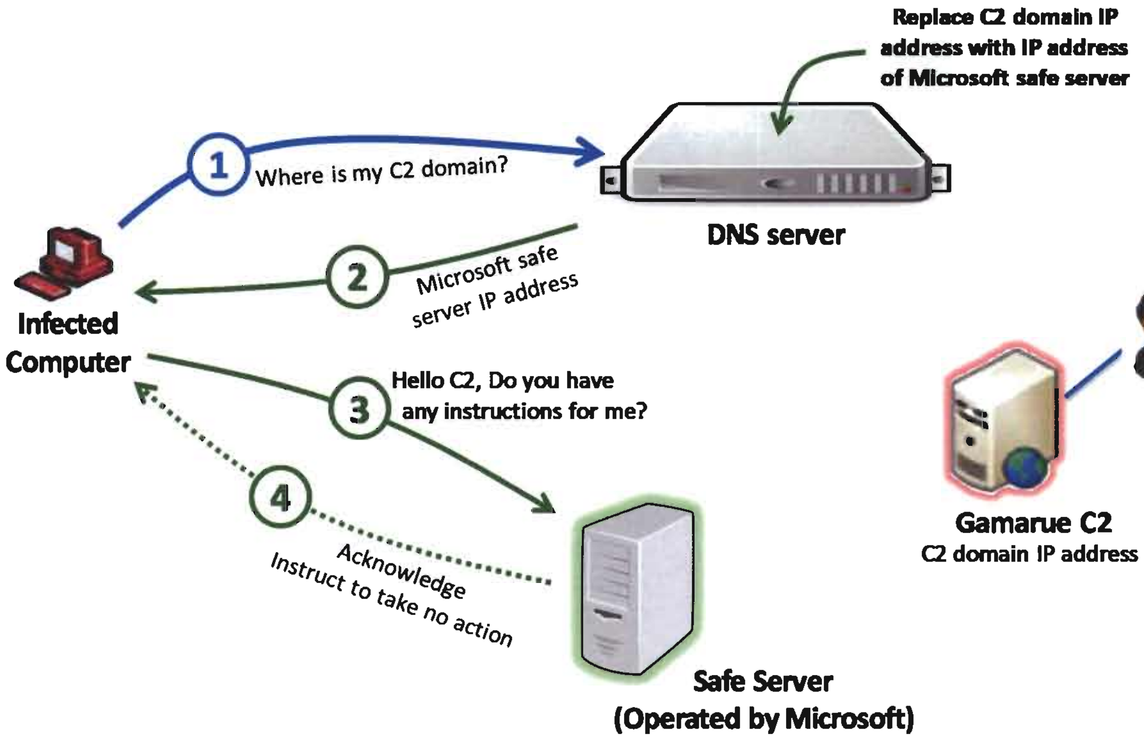
Replace C2 domain IP address with IP address of Microsoft safe server
1
Where is my C2 domain?
DNS server
2
Microsoft safe server IP address
Infected Computer
3
Hello C2, Do you have any instructions for me?
4
Acknowledge
Instruct to take no action
Gamarue C2
C2 domain IP address
Safe Server (Operated by Microsoft)

Fig. 4

[3] Additionally, this will allow Microsoft to identify and assist customers regarding remediation of other malware delivered by Gamarue, stopping the harm related to this additional malware.

24. In step 1 of **Figure 4**, above, an infected computer contacts a DNS server and requests the IP address that corresponds to the C2 server domain that has been programmed into the Gamarue malware. But now, the DNS server will instead respond with the IP address for a Microsoft safe server, as shown in step 2 of **Figure 4**, above. The infected computer will then contact the Microsoft safe server, as shown in step 3 of **Figure 4**, above. Finally, as shown in step 4 of **Figure 4**, above, the Microsoft safe server acknowledges the infected computer's contact and instructs the infected computer not to take any malicious action at this time.

25. The relief described above can be implemented by directing the third-party registry services listed in **Exhibit 2** to this declaration (and **Appendix A** to the Complaint) to associate the Gamarue C2 server domains in **Appendix A** with Microsoft-controlled name servers, NS66.microsoftinternetsafety.net and NS67.microsoftinternetsaftey.net. This relief is requested in the proposed TRO and preliminary injunction.

I declare under the 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 13th day of November, 2017.

Vishant Patel

Vishant Patel

Professional Experience

Microsoft Corp. – Redmond, WA

Digital Crimes Unit **August 2012 - Present**
Senior Manager of Investigations

- Developed, implemented, and managed investigations regarding botnets, malware and computer intrusions impacting Microsoft and its customer, products, and services.
- Developed evidenced and participated in legal actions directed at identifying and disabling botnet infrastructure.
- Responded and investigated the System & Network incidents.
- Evaluated and implemented Security Event Management (SEM), Forensic and Incident Management technologies.
- Communicated Cyber tools, techniques, & procedure internally and external groups.
- Acted as liaison with local, federal, and international law enforcement and industry groups in prosecuting organized crime groups.

Citigroup Inc - New York, NY

Cyber Investigation & Response Team **February 2011 - Present**
Senior Investigator / Vice President

- Developed, implemented, and managed enterprise level Anti-Phishing & Anti-Trojan solutions to meet Citi framework. These solutions anticipate all aspect of Phishing & Trojan threats and takes systematic counter measures to mitigate threats.
- Participated in development of new group called Citi Cyber Intelligence Centre (CIC). CIC collects, analyzes, and exchanges actionable Cyber intelligence that increases threat awareness and decrease risk posture.
- Responded and investigated the System & Network incidents involving DDoS, Advance Persistent Threat (APT), ZERO day, Policy Violation, & Data leakage.
- Advised monthly and on ad hoc basis about Cyber threats to Senior Management by performing Risk Assessments on CIRT incidents.
- Interacted with Information Technology Risk Management group to mitigate gaps identified within the process and technology controls through CIRT investigation.
- Managed third party security vendors to ensure they are in compliance with Citi policies, standards, procedures, and service level agreements.
- Evaluated and implemented Security Event Management (SEM), Network Forensics', and Incident Management technologies.
- Communicated Cyber tools, techniques, & trends on vetted information sharing groups such as FS-SIAC, DPN, UK Payment Councils, FIRST, & Botnet take-down task force.
- Acted as liaison with local, federal and international law enforcement and industry groups in prosecuting organized crime groups.
- Participated in working groups to update Citi information security policies, standards, and procedures involving CIRT components.
- Developed & conducted Cyber investigation training to Investigators & new hires.
- Managed team of three individuals to ensure CIRT investigation meets industry best practices.
- Interacted with Citi fraud risk group in development of multilayered risk strategies to mitigate emerging social engineering, online banking, mobile, and carding fraud.
- Acted as liaison with forensics, vulnerability assessment, intrusion detection, and anti-virus group to mitigate Zero day vulnerabilities impacting Citi globally.

Vishant Patel

Cyber Investigation & Response Team **February 2005 – February 2011**
Investigator / Assistant Vice President

- Designed and implemented controlled lab environment to perform runtime and reverse engineering of Malware.
- Developed and automated customized parsing scripts to extract and normalize the compromised credentials captured by Phishing and Malware.
- Developed a self service portal to disseminated compromised credentials to respective fraud risk group in real time.
- Published routine comprehensive intelligence reporting of internal and external Cyber threats to Citi businesses.
- Developed strategic partnership with ICANN & Internet Service Provider to detect and mitigate Phishing & Malware threats.
- Advised Security Operation Center in development of framework to detect and track emerging Cyber threats.

CompUSA – New York, NY

Lead Network & Computer Technician **January 2000 - February 2005**

- Acted as a network team lead in migration and integration of New York stores.
- Configured and deployed store Point of Sale systems.
- Designed and implemented secured WiFi networks.

CERTIFICATIONS

- Malware Artifacts 2006
- XANALYS Link Explore
- A+ Technician

Programming Languages

- C++
- Java
- HTML
- SQL
- Perl
- Python

Operating System

- Windows
- OS X
- Linux
- Andorid

Application / Appliances

- i2 Workbench
- SharePoint
- Office
- ArcSight
- Netwiness
- Source Fire

Personal Accomplishments

Certificate of Appreciation from Federal Bureau of Investigation

APPENDIX A

.COM Registry

VeriSign, Inc.
VeriSign Information Services, Inc.
VeriSign Global Registry Services
12061 Bluemont Way
Reston Virginia 20190
United States

.COM Domains

Domain	Registrant E-mail
cabinme24hrs.com	ishad2022222@gmail.com
joojlee.com	contact@whoissecret.org
produkktc.com	ishad2022222@gmail.com
starmanspo.com	jad.dodo1@gmail.com
windowsupdate-microsoft.com	the-schwarz@linuxmail.org

.INFO Registry

Afilias USA, Inc.
300 Welsh Road, Building 3
Suite 105
Horsham Pennsylvania 19044
United States

Afilias Limited
Afilias plc
4th Floor, International House
3 Harbourmaster Place
IFSC, Dublin D01 K8F1
Ireland

.INFO Domains

Domain Name	Registrant E-mail
dertyert.info	dertyert.info@regprivate.ru