**Kennesaw State University**
**DigitalCommons@Kennesaw State University**

KSU Proceedings on Cybersecurity Education, Research and Practice

2017 KSU Conference on Cybersecurity Education, Research and Practice

# Voice Hacking Proof of Concept: Using Smartphones to Spread Ransomware to Traditional PCs

Leonardo I. Mazuran
*University of North Georgia*, limazu0873@ung.edu

Bryson R. Payne
*University of North Georgia*, bryson.payne@ung.edu

Tamirat T. Abegaz
*University of North Georgia*, tamirat.abegaz@ung.edu

Follow this and additional works at: https://digitalcommons.kennesaw.edu/ccerp


Part of the Information Security Commons, Management Information Systems Commons, and the Technology and Innovation Commons

Mazuran, Leonardo I.; Payne, Bryson R.; and Abegaz, Tamirat T., "Voice Hacking Proof of Concept: Using Smartphones to Spread Ransomware to Traditional PCs" (2017). *KSU Proceedings on Cybersecurity Education, Research and Practice*. 4.
https://digitalcommons.kennesaw.edu/ccerp/2017/practice/4

This Event is brought to you for free and open access by the Conferences, Workshops, and Lectures at DigitalCommons@Kennesaw State University. It has been accepted for inclusion in KSU Proceedings on Cybersecurity Education, Research and Practice by an authorized administrator of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

**Abstract**
This paper presents a working proof of concept that demonstrates the ability to deploy a sequence of hacks, triggered by speaking a smartphone command, to launch ransomware and other destructive attacks against vulnerable Windows computers on any wireless network the phone connects to after the voice command is issued. Specifically, a spoken, broadcast, or pre-recorded voice command directs vulnerable Android smartphones or tablets to a malicious download page that compromises the Android device and uses it as a proxy to run software designed to scan the Android device's local area network for Windows computers vulnerable to the EternalBlue exploit, spreading a ransomware-like application to those PCs, and executing it remotely. In addition to describing the proof-of-concept attack in detail, the authors propose several remedies individuals and organizations can use to prevent such attacks.

**Disciplines**
Information Security | Management Information Systems | Technology and Innovation

This event is available at DigitalCommons@Kennesaw State University: https://digitalcommons.kennesaw.edu/ccerp/2017/practice/4

# EXTENDED ABSTRACT

In this paper, we present a working proof-of-concept attack that demonstrates the ability to use voice commands on Android smart phones as a vector to hijack a user's Android device and use it to scan for and exploit vulnerable Windows PC's on any wireless network the phone may touch. Our proof of concept makes novel use of a combination of two Android vulnerabilities and one Windows vulnerability to successfully compromise traditional PCs using an Android mobile device for both reconnaissance to identify the victim PCs and delivery of the malware through the victim's network.

We have developed a multi-step "kill chain" activated by a voice command or hyperlink, to exploit vulnerable Android devices across two different major versions of the Android OS, turning them into scanners searching for the EternalBlue Windows file-sharing vulnerability on any laptop, desktop, or workstation attached to the same network as the Android mobile device. The Android device is then used as a proxy to maintain a connection between discovered PCs and the malware server(s), which can exploit the EternalBlue SMB vulnerability and remotely deploy ransomware or other arbitrary executable code on victim PCs.

Specifically, this attack allows a spoken, broadcast, or pre-recorded voice command to direct vulnerable Android smartphones or tablets to a malicious download page that compromises the Android device and uses it as a proxy to run software designed to scan the Android device's local area network for Windows computers vulnerable to the EternalBlue exploit, spreading a ransomware-like application to those PCs, and executing it remotely.

In addition to describing the proof-of-concept attack in detail, the authors propose several remedies individuals and organizations can use to prevent such attacks. For individuals, restricting or disabling voice services and maintaining up-to-date security patches for both their mobile devices and desktop/laptop computers is a first line of defense. For organizations, a layered approach to security, including proper network and data segmentation, applying security updates for company-owned devices and requiring updates for any personal devices before allowing them to connect to company networks, and actively monitoring suspicious traffic or behavior from connected mobile and IoT devices are keys to preventing the types of attacks described in this work.