go-Raider: Managing Cyber-Resilient Botnets through Blockchain

Dimitri Kamenski*, Arash Shaghaghi*, Matthew Warren*, Salil S. Kanhere‡
*Deakin University, Geelong, Australia – Centre for Cyber Security Research and Innovation,
†RMIT University, Melbourne, Australia
‡The University of New South Wales (UNSW Sydney), Australia
{c.riveraalvarez,salil.kanhere}@unsw.edu.au
a.shaghaghi@deakin.edu.au

***Abstract*—We showcase how attackers can leverage decentralised technologies to dynamically manage trust requirements in illicit activities. We focus on controlling botnets that are resilient to hostile takeovers. We present a step-by-step demo of how blockchain-based botnets can be built focusing on Bitcoin blockchain. We also show how specific Bitcoin APIs can be used in order to write extraneous data to the blockchain. Finally, we discuss possible defence mechanisms against the attack presented.**

I. Overview

This demo is based on a recently published article entitled as ‘Attacking With Bitcoin: Using Bitcoin to Build Resilient Botnet Armies’ [8]. Our demonstration exposes a critical threat, the concept of a dynamic censorship-resistant trust chains. Malicious activity between two or more parties often relies on trust, through the continuity of identity. Whilst conducting malicious activities online, bad actors can go to extreme lengths to avoid censorship. This demo suggests that there is avid reason behind monitoring and surveillance of public blockchain users. This dynamic trust chain provides the ability for these adversaries to continue doing business in spite of serious censorship resistance. In our demonstration we show how this protocol allows an attacker to harden a botnet army against takeovers, government intervention and cloud server shutdowns. However, the same attacks can be abstracted to maintain trust between buyers and sellers of illicit paraphernalia during darknet server raids. If a server is taken down, the buyers and sellers are able to renegotiate trust in similar ways to how our proposed demonstration of botnets can reestablish trust with a Command & Control center.

Here, we assumes that the attacker has entered the ‘post-exploitation’ phase, meaning an initial payload has successfully loaded onto the chosen victim. In the case of the Mirai botnet, there was an estimated 600,000 devices infected, maintained and controlled by a single botnet master [3]. The large number of devices under control of botmasters and the financial implications involved, makes post-exploitation a critical aspect of cyber attacks. As the complexity of an attack grows, so does the demands on an attackers skill to manipulate bots through adverse communication problems. This includes handling severed connections.

In order to improve the resiliency of a botnet, botmasters deploy more sophisticated and ‘dynamic’ communication methods with ‘floating C&C servers’ [9].Throughout the last 10 years various botnets such as Conficker, Kraken and Torpig leaned on domain fluxing, which involves pre-determined DNS addresses that are cycled by the malware until a successful connection is made [13]. By registering these pre-determined DNS addresses researchers were able to conduct a full takeover of the Torpig DNS-fluxing botnet [5]. A unique case where a famous popstar’s Instagram comments were used to control malware show just how desperate attackers might get to obscure processes, defend bots and control their malicious attacks through third party interactions [1]. These methods are an indication that malware designers are conscious that their attacks have a single point of failure, which is the C&C server’ [11].

Blockchains provide a means to avoid these limitations. They have been sold to the general public, all under the guise of the importance of ‘censorship resistance’. However, truly censorship resistant networks are a serious threat and may be exploited by malicious actors. We showcase this through the effects of blockchain transactions on malware communication protocols. Malware typically relies on a centralised source of truth for communication of remote procedure calls and instruction sets. This centralised truth is a critical weakness. In dire situations, government intervention can shut down certain malware command and control centers hosted in cloud infrastructure using existing legal avenues. These situations could arise if malware cannot be removed in a timely manner, control flow cannot be diverted or we are unsure of the extent of damage caused to other people who may have encountered this malware.

We have managed to read arbitrary data from the blockchain. For this, we return transactions within a given range by emulating the behaviour of a full node and communicating directly with other Bitcoin full nodes. We directly request a list of actual blockchain data, our malware then begins to analyze these transactions for instruction information. The control plane for this type of attack can be considered resilient against existing countermeasures adopted by ISPs and governments.

We discuss the implications of this research, how and where we should go from here and most interestingly we critically analyze the OP_Return code usage providing insights on how this is being used in the real world. We will look through some statistical analysis of OP_Return and a thematic analysis to gauge trends and provide insight as to why we believe this to be of critical importance to future malware researchers.

II. Demonstration Details

A. Scope

The network architecture and communication flow of our setup can be visualised in Fig 2 and Fig 1. We aim to showcase how our attack works by breaking it down into the following categories:

1) Build: How to establish dynamic shells
2) Control: How to write arbitrary data to the Bitcoin blockchain
3) Maintain: How to read arbitrary data from the Bitcoin blockchain
4) Analysis and Prevention: Discuss the prevalence of this threat and how prevention might work.

B. Equipment

We will be using a single laptop with the following software installations; VMware Workstation 16 running Windows 10 Evaluation and Kali Linux, Bitcoin Core, Metasploit Framework.

C. Novelty

Some researchers believe that peer-to-peer botnets appear to be more superior at defending against takeovers or shutdowns, however, they are "subject to a unique class of attacks such as node enumeration and poisoning" [10]. They are susceptible to random node failures and disinfection strategies (such as monitoring and blacklisting peer lists) [7]. If the communication between a single peer-to-peer botnet is compromised or spoofed the whole network may be compromised. Aspects of peer-to-peer botnets can be leveraged, whilst minimising the risks exposed through centralised Command & Control Servers (C&C servers). Omer Zohar provides an example of blockchain-based botnets, with a focus on obtaining full RPC based instruction sets, delivered through blockchain transactions [14]. Zohar's 'Unstoppable chains' explains in detail, with smart contract examples, on how Ethereum (a similar protocol to Bitcoin) can be used to manipulate the behaviour of botnets [14]. However this is an expensive, profit-leaking action. As seen in figure 1, we show a different slant on the same attack by using the blockchain to provide the location and details of the C&C server to the bot.

The foundation of our demo includes, how to produce dynamic shell sessions, write arbitrary data to the blockchain, and how to emulate full nodes in order to read arbitrary data from the blockchain. Although our demo provides a simple IP for our malware to reconnect to, the demo itself will discuss some more covert and creative ways attackers may expand on these concepts. The capabilities and possible directions this attack could manifest enforces its superiority against other blockchain based botnets. We are confident that the demo will draw a light to the critical components of blockchain that pose real world tangible threats to our cyber security practices.

III. Research Overview

As mentioned, this demonstration is based on our recently published paper [8]. In this paper, we discussed censorship resistant malware in detail and covered several areas that we aim to demonstrate during the demo.

This novel attack is based on the Bitcoin blockchain, which was popularized as an alternative to the global financial system [8]. As an immutable ledger, it acts as a censorship resistant append-only database. This database is aimed at recording who owns what bitcoin [4]. Bitcoin is also capable of storing non-Turing complete actions, consisting of up to 80 bytes of arbitrary data, allowing us to store permanent instruction for our malware on this immutable ledger [8].

In order to produce dynamic shells, we initially leveraged the Metasploit Framework (MSF) and the protocol in MSF to manage staged payloads. This dynamic shell injected python code into the victim that facilitated low level TCP communication with known Bitcoin full nodes in order to extract transactions and determine instruction sets. The instruction we used contained single IP addresses inside of the Bitcoin OP_Return script codes, which usually holds 'arbitrary data'. We then used that IP address in order to reconnect to a new host in the event that the original host was taken down. This process can be seen in Fig 1. Along side this process is a simple script we prepared in order to write arbitrary data to the Bitcoin blockchain. The final result of these moving parts is a piece of malware that does not rely on any centralised source for collecting instruction sets. As mentioned above we have since detracted from MSF and are now using our own custom post-exploitation framework.

The research also discusses the future implications. Specifically, how criminals may 'abstract' the protocol into a generic 'trust chain' protocol. This would make it difficult to shut down illicit activities that rely on trust to establish ongoing communication. An example provided earlier, is a darknet drug store being taken down. As in the case of the malware, trust can be reestablished through blockchain transactions. Rather than word of mouth, a new store can be opened in different locations that provably belong to the existing owner. Arbitrary data stored on blockchain can facilitate the on going relationships between criminals in the community. This is a very real and active threat that we believe our demo will raise awareness about. The motivation behind this research was to promote further investigations on post exploitation. We hope to reduce the number of avenues an attacker can pursue through the exploration and understanding of these modern post-exploitation vectors.

IV. Countermeasures

Existing countermeasures may be employed to flag infected devices, and highlight anomalies in communication channels [12] [2]. Botmark defines C-flows as traffic that share the same protocol, source IP, destination and port within an epoc [12]. They then provides the basis for statistical analysis to suggest that C-flow anomalies can lead to a 99.94% detection rate of botnets [12]. Research surrounding similar floating C&C

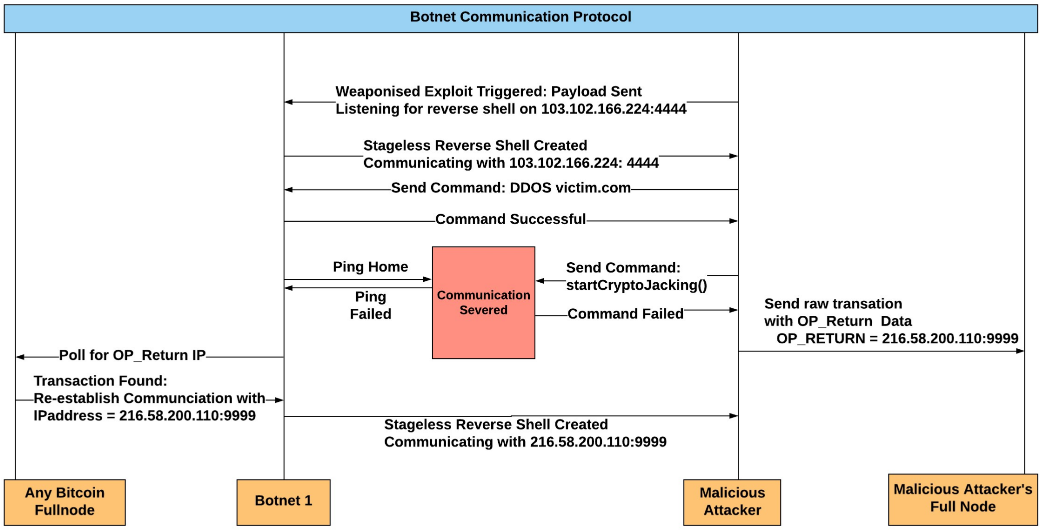
Botnet Communication Protocol
Weaponised Exploit Triggered: Payload Sent
Listening for reverse shell on 103.102.166.224:4444
Stageless Reverse Shell Created
Communicating with 103.102.166.224: 4444
Send Command: DDOS victim.com
Command Successful
Ping Home
Ping Failed
Communication Severed
Send Command: startCryptoJacking()
Command Failed
Send raw transation with OP_Return Data
OP_RETURN = 216.58.200.110:9999
Poll for OP_Return IP
Transaction Found:
Re-establish Communciation with
IPaddress = 216.58.200.110:9999
Stageless Reverse Shell Created
Communicating with 216.58.200.110:9999
Any Bitcoin Fullnode
Botnet 1
Malicious Attacker
Malicious Attacker's Full Node

Fig. 1. Botnet Communication Protocol Diagram: Details how the botnet communicates directly with the attacker

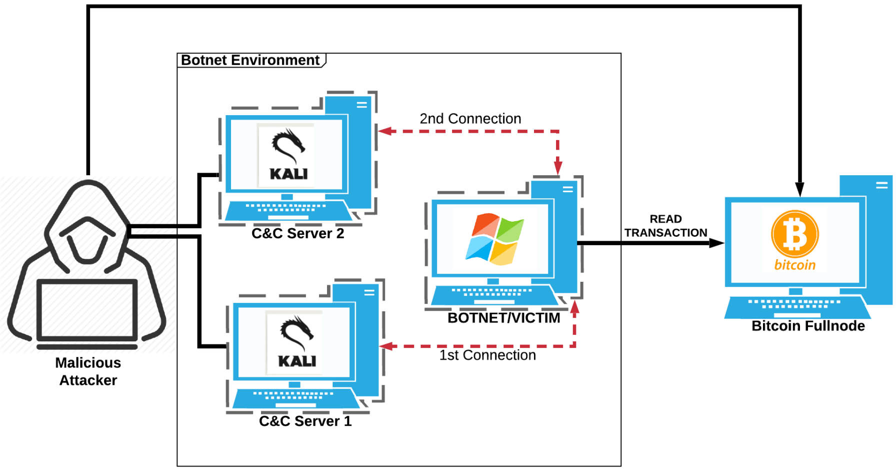

Fig. 2. High-level Architecture of our proof of concept implementation

botnets, suggested the monitoring of DNS queries may have resulted in a 99.35% detection rate of Zeus and Citadel's Conficker DNS based botnet [2]. Similarly, in order to query for information and we must make requests through the relevant Bitcoin Protocol. These requests can be tracked on local networks to flag potentially infected devices.

Furthermore, the uniqueness of this attack vector suggests we may have a higher degree of likelihood in connecting these attacks to physical people. In order to emulate fullnodes we are required to use JSON-RPC APIs, these inevitably force attackers who are leveraging this communication protocol to broadcast an IP address. We believe that monitoring of all IP addresses posting arbitrary data to Blockchains is an essential preventative measure. Kaminsky highlights how IP monitoring of full nodes [6], may assist law enforcement agencies in linking these IP addresses and Bitcoin transactions to physical people. Finally Bitcoin's do not just represent arbitrary data, they hold real wealth and people may make mistakes in the real world when handling funds used to control these illicit communication channels.

V. Conclusion and Future Work

We have highlighted that Bitcoin's OP_Return is can be weaponized into a critical threat that can be leveraged by a sophisticated attacker. As such, we believe that it is warranted, to implement monitoring procedures and provide general threat intelligence capabilities to organisations that may be at risk from decentralised botnets.

References

[1] "Britney spears: Malware planted in singer's instagram page," Jun 2017. [Online]. Available: https://www.bbc.com/news/technology-40200400

[2] K. Alieyan, A. Almomani, M. Anbar, M. Alauthman, R. Abdullah, and B. B. Gupta, "Dns rule-based schema to botnet detection," *Enterprise Information Systems*, vol. 0, no. 0, pp. 1–20, 2019. [Online]. Available: https://doi.org/10.1080/17517575.2019.1644673

[3] E. Bursztein, "Inside mirai the infamous iot botnet: A retrospective analysis," 2017.

[4] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[5] M. Cova, R. Kemmerer, G. Vigna, C. Kruegel, B. Gilbert, and B. Stone-Gross, "Analysis of a botnet takeover," *IEEE Security Privacy*, vol. 9, no. 01, pp. 64–72, jan 2011.

[6] Dan Kaminsky, "Black Ops of TCP/IP 2011." [Online]. Available: https://dankaminsky.com/2011/08/05/bo2k11/

[7] C. R. Davis, S. Neville, J. M. Fernandez, J.-M. Robert, and J. McHugh, "Structured peer-to-peer overlay networks: Ideal botnets command and control infrastructures?" in *Computer Security - ESORICS 2008*, S. Jajodia and J. Lopez, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 461–480.

[8] D. Kamenski, A. Shaghaghi, M. Warren, and S. S. Kanhere, "Attacking with bitcoin: Using bitcoin to build resilient botnet armies," in *13th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2020)*. Springer Nature, p. 3.

[9] E. C. Ogu, O. A. Ojesanmi, O. Awodele *et al.*, "A botnets circumspection: The current threat landscape, and what we know so far," *Information*, vol. 10, no. 11, p. 337, 2019.

[10] C. Rossow, D. Andriesse, T. Werner, B. Stone-Gross, D. Plohmann, C. J. Dietrich, and H. Bos, "Sok: P2pwned - modeling and evaluating the resilience of peer-to-peer botnets," in *2013 IEEE Symposium on Security and Privacy*, 2013, pp. 97–111.

[11] P. Wang, B. Aslam, and C. C. Zou, "Peer-to-peer botnets," in *Handbook of Information and Communication Security*. Springer, 2010, pp. 335–350.

[12] W. Wang, Y. Shang, Y. He, Y. Li, and J. Liu, "Botmark: Automated botnet detection with hybrid analysis of flow-based and graph-based traffic behaviors," *Information Sciences*, vol. 511, pp. 284–296, 2020.

[13] S. Yadav, A. K. K. Reddy, A. L. N. Reddy, and S. Ranjan, "Detecting algorithmically generated domain-flux attacks with dns traffic analysis," *IEEE/ACM Transactions on Networking*, vol. 20, no. 5, pp. 1663–1677, 2012.

[14] Zohar O., "Unblockable Chains – a poc on using blockchain as infrastructure for malware operations," [Accessed: 01.02.2020]. [Online]. Available: https://github.com/platdrag/UnblockableChains