North Korea Targeted South Korean Cryptocurrency Users and Exchange in Late 2017 Campaign

By Juan Andres Guerrero-Saade and Priscilla Moriuchi

Appendix A

Indicators of Compromise

Lures

MD5	SHA256
da02193fc7f2a628770382d9b39fe8e0	3cfc7666c97c38f38a3b3ec1d132f2836ade7e6e6e3cddb30b0d7d81682de0b2
3d0d71fdedfd8945d78b64cdf0fb11ed	3e9eab029c52ac34b91f906c8f92ad9059531f825905260023764f8a069edbbf
63069c9bcc4f8e16412ea1a25f3edf14	396a684949c96815b54c8e4c2fafbe6324d8c4dde2c9294411658fb5209cd70c
8152e241b3f1fdb85d21bfcf2aa8ab1d	1cc7ad407fc87acb9c961105943c87a7bd77c4d4cc90b84b46fb5dcf779b50fd

Payloads

46d1d1f6e396a1908471e8a8d8b38417	3368b6060d181e39a57759ab9b7f01221e0cd3a397000977aa8bb07a0e6a94ca
6b061267c7ddeb160368128a933d38be	ca70aa2f89bee0c22ebc18bd5569e542f09d3c4a060b094ec6abeeeb4768a143

afa40517d264d1b03ac5c4d2fef8fc32	f94fb5028a81177bb5ea3428349da4d9b125f81adb658df40d6e8f3ea0e0e3e7
c270eb96deaf27dd2598bc4e9afd99da	cf065e50a5bef24099599af6a60a78c1607a04b21d3573a25ab26bf044a119d6
d897b4b8e729a408f64911524e8647db	5afa8329c0a159811b55c92303f0d0b9b8834843c76f51777593d414bda5191b
e1cc2dcb40e729b2b61cf436d20d8ee5	77cee0ccc739d3d420e95460c72f7ad2a9846f06e4a7089fb92b8fca4a52ce3f

Command-and-Control

110.173.188.53:443
70.60.36.183:443
72.10.122.70:443
112.160.75.159:5443
125.142.192.81:443
175.213.42.234:443

Yara Rules

```
rule apt_NK_Lazarus_SKOlympics_EPS
{
	meta:
		author = "JAG-S, Insikt Group, RF"
		desc = "CN terms in PostScript loader"
		TLP = "Green"
		version = "1.0"
		md5 = "231fe349faa7342f33402c562f93a270"

	strings:
		$eps_strings1 = "/yinzi { token pop exch pop } bind def" ascii wide
		$eps_strings2 = "/yaoshi <A3E6E7BB> def" ascii wide
		$eps_strings8 = /\/yaoshi <[A-F0-9]{8}> def/ ascii wide
		$eps_strings3 = "/yima{" ascii wide
```

```
            $eps_strings4 = "/funcA exch def" ascii wide
            $eps_strings5 = "0 1 funcA length 1 sub {" ascii wide
            $eps_strings6 = "/funcB exch def" ascii wide
            $eps_strings7 = "funcA funcB 2 copy get yaoshi funcB 4 mod get xor put"
ascii wide

      condition:
            6 of them
}
```

```
rule apt_NK_Lazarus_Fall2017_payload_minCondition
{
    meta:
        desc = "Minimal condition set to detect payloads from Fall 2017 Lazarus
Campaign against Cryptocurrency Exchanges and Friends of MOFA 11"
        author = "JAGS, Insikt Group, Recorded Future"
        version = "2.0"
        TLP = "Green"
        md5 = "46d1d1f6e396a1908471e8a8d8b38417"
        md5 = "6b061267c7ddeb160368128a933d38be"
        md5 = "afa40517d264d1b03ac5c4d2fef8fc32"
        md5 = "c270eb96deaf27dd2598bc4e9afd99da"
        md5 = "d897b4b8e729a408f64911524e8647db"
        md5 = "e1cc2dcb40e729b2b61cf436d20d8ee5"

    strings:
        $sub1800115A0 =
{488D542460488D8DB005000041FF9424882000004C8BE84883F8FF0F84EA010000488D8DC007000033D
241B800400000E8}
        $sub18000A720 = {33C0488BBC2498020000488B9C2490020000488B8D600100004833CCE8}

    condition:
        uint16(0) == 0x5A4D and filesize < 5MB
        and
        any of them
}
```