New Advanced Persistent Threat (APT) Dark Caracal

Alex Tarter and Gurbir Singh
Thales Cyber & Consulting

Threats, Persistent Threats and Advanced Persistent Threats.

If someone out there really wants your data, they will eventually get it. An Advance Persistent Threat is Advanced (employ leading edge cyber techniques and technologies), Persistent (additional resources financial or personnel as required) Threat that keeps hammering away in the background quietly acquiring data without the owners knowledge.

What is an Advance Persistent Threat?

An advance persistent threat is a sophisticated cyber activity supported by a nation state to compromise a high value target. Attacks of this nature are stealthy, can persist for months or years and are discovered long after the compromise has taken place if at all,

Discovery of Dark Caracal

A report published on 18th January 2018 announced the discovery of an Advanced Persistent Threat (APT) conducting Cyber Espionage on a global scale since at least 2012. An extensive investigation by the security company Lookout and the civil rights organisation – the Electronic Frontier Foundation (EFF) have identified a command and control infrastructure used to generate test and distribute malware.

This group targets both windows and mobile Android platforms. The sophisticated malware has targeted thousands of mobile devices belonging to journalists, military personnel, lawyers, activists and educational institutions. Overtime it has extracted hundreds of gigabytes of private data including sms messages, call records, audio recordings and photos from user devices in at least 21 countries including Europe and North America.

Social Engineering and Spear-Phishing techniques were used to acquire the targets. Dark Caracal servers hosted phishing sites, which look like login portals for familiar services such as Twitter, Google and Facebook. Users were lured by public posts on current affairs and political themed news stories containing links to these fake sites in relevant Facebook groups, Twitter hash tags and Whatsapp groups.

Dark Caracal Infrastructure

The investigation revealed that the Dark Caracal infrastructure is large, sophisticated and growing. Initially the infrastructure was primarily used to attack windows users but has evolved to a point today where most of its 48GB data is from mobile devices and 33GB from Windows. The report identified 11 versions of familiar Android apps compromised with the Pallas malware that allows an infected device to be accessed remotely without the knowledge of the owner. Phishing campaign enticed users to download these compromised versions of the apps to their mobile devices. The apps included Signal, Whatsapp and Plus Messenger. All infected apps were fully functioning and found only on the Dark Caracal infrastructure. Users accessing the uninfected apps from the official Android App store were not impacted.

The infrastructure is hosted on an off-shore hosting company Shinjiru headquartered in Malaysia. Shinjiru offers a number of services including "bullet proof" hosting which allows its customers to host any type of content whilst protecting their identity and takes payment in Bitcoin.

The infrastructure consists of

- Watering Hole Server – hosts the malicious apps developed using the Pallas malware. Pallas gets on to a user's mobile device that the user has unwittingly (by clicking on a phishing link) installed and given admin privileges to as part of the installation process. Once the mobile device is infected, it can be controlled by the primary command and control server.
- Phishing domains – two fake but realistic looking login webpages were identified. One designed to mimic Twitter and another for Facebook to collect user credentials.
- Primary command and control server - used to connect to devices once successfully compromised.
- Command and control servers for Windows devices that hosted control panels for multiple campaigns using a variety of malware, Remote Access Trojans (IRIS, RAT, Bandook and AcornRAT were detected) that allows the command and control servers to remotely access the infected windows device.
- Support and admin personnel - Email addresses, names and telephone numbers were recorded of individuals involved in support and administration of the infrastructure.

The report lists over 90 Indicators of Compromise (IOC) consisting of 11 associated with Android malware, 26 instances of malware for Windows, Linux and Mac and 60 domain/IP based IOC. The Lookout-EFF investigation detected multiple unrelated and overlapping campaigns indicating that the Dark Caracal infrastructure has been in place since around 2011 has evolved and is shared by multiple actors targeting specific victims. The operations and campaigns were still active up to December 2017.

The impact

Once the users' devices were compromised, functions with the Pallas spyware allowed the Dark Caracal operators to manually trigger or automatically schedule download of user data which included text messages, contacts, physical location using longitude and latitude from the GPS and harvest login credentials. Owners of compromised devices could be monitored by activating their

camera, microphone and capture screen. The malware functions also allowed files to be deleted from the mobile device, uploaded to the mobile device, initiate audio recording and take photos with front or rear camera and downloaded to the Dark Caracal servers.

The analysis of stolen data arriving at the controlling servers revealed infected user devices in 21 countries including France, US and Germany. Android devices accounted for 48GB of the stolen data which comprised of SMS texts (32.4%), data files (17.6%), contacts (16.9%), call records (10%) and unique wifi SSIDs 13.8%. The files consist of photos, Skype log database, IPhone backups and corporate legal documents. The report does not identify the individual victims.

APTs are sponsored by nation-states and receive high levels of political and financial support to produce sophisticated tools for covert cyber-attacks. Authoritative attribution of a cyber-attack is difficult. In this instance the investigators have identified IP addresses, email addresses used to register domains within the campaign and wifi SSID that have a clear connection to the headquarters of the General Directorate of General Security (GDGS) in Beirut, Lebanon.

Protecting against Dark Caracal

In a real sense, protecting against threats which are inherently advanced and persistent may not ultimately be possible. Senior management should ensure that their business has the resources and high level commitment to managing security risk as a business objective. Security should not be seen as an expense but as an investment. An information security management system consists of structures, policies and process for governance, risk management and compliance. Some of the key steps to mitigate risks of access to unauthorised user data include

- Enforce mandatory regular cyber security training for all employees not just the initial induction.
- Deploy two factor authentication wherever practical.
- Limit the number and types of internet facing connections
- Incorporate Network Detection, Network Protection, event alerting and reporting solutions
- Record, monitor and regularly review event logs
- Undertake annual IT health checks or Pentest in addition to regular internal security audit programme for all key systems interfaces, services and applications.
- Limit administrative access to user devices restricting the applications and the access levels to only those required by the users to perform their roles.
- Implement a regime for regular backup, patching, antivirus and network monitoring.
- Ensure user access is limited to what they require i.e. the principles of Least Privilege and Need to Know.
- Implement a security incident management process to limit the impact of potential incidents and learn from them.

The National Cyber Security Centre offers advice and support on cyber security matters including guidance for small businesses and home users via informative blog posts, useful info graphics, a comprehensive Glossary, a weekly threat report and Incident management.

Thales Cyber and Consulting Services

Thales is a global security company with distinguished track record in designing, building and protecting complex systems serving the aerospace, automotive and industrial sectors. Current services offered include

Cyber Vulnerability Investigation (CVI): Understand the effectiveness of existing security controls protecting IT systems

Thales's Cyber Human Error Assessment Tool (CHEAT): A cost-efficient process for determining how human vulnerabilities, psychological motivations, and cultural issues might weaken an organisation's cyber security .

General Data Protection Regulation (GDPR): Understanding what needs to be done to achieve compliance.

Cyber HealthCheck: Provide valuable information to inform strategic and tactical decision making for mission-critical systems and organisations.

Thales Security Operations Centre (SOC): A comprehensive Protective Monitoring service available on a flexible deployment and Service Level Agreement options.

Thales Intelligence Services (TIS): Generating intelligence to inform safety and security critical decision making.

Thales Risk Assessment Process (TRAP): A unique Thales risk assessment product for interconnected Industrial Automated Control Systems (IACS) across the Enterprise.

Details on these services including datasheets, white papers, and brochures are available here or via email **thalescyberandconsulting@uk.thalesgroup.com**

Dark Caracal Technical Report	https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf
Electronic Frontier Foundation	https://en.wikipedia.org/wiki/Electronic_Frontier_Foundation https://www.eff.org/
Advance Persistent Threats	https://www.symantec.com/theme.jsp?themeid=apt-infographic-1 https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html
National Cyber Security Centre	https://www.ncsc.gov.uk/guidance
Thales Cyber and Consulting	https://www.thalesgroup.com/en/countries/europe/united-kingdom/security/thales-cyber-consulting/cyber-services

Thales Cyber & Consulting

Thales is a global security company with a strong global presence and particular expertise in designing, building and protecting complex systems. We are committed to helping organisations

understand the threats to their businesses and are a major collaborator with the National Cyber Security Centre in the UK.

Since 1989, Thales Cyber & Consulting have been delivering the highest standard of technical and business change consultancy to clients who work in the most complex technical and regulated environments. We have recently refined and re-launched our range of consultancy service offers to provide your organisation with targeted solutions. We recognise that every client is different and that sectors are increasingly overlapping; that is why we never simply offer off-the-peg solutions, but rather listen to how we can add value to your delivery and development goals. We bring together consultants specialised in cyber security, safety, systems engineering, business change, human factors and training.

Our services range from architecture and secure-by-design solutions for the development of new services, systems and products, to cyber health-checks and support for certification, trust management and ensuring compliance with the new GDPR data protection regulations of new and existing systems. We also offer on-going security monitoring services from our Security Operations Centre (SOC) and our innovative Thales Risk Assessment Process (TRAP) to ensure your organisation is ready to withstand the next cyber-attack.

For more information visit our website at http://www.thalesgroup.com/en/tcc-uk or email thalescyberandconsulting@uk.thalesgroup.com