Printer 535218
[or 29535218]
on May 9, 2017
at 6:20 am
(Reality Leigh Winner)

[redacted] DIRNSA

National Security Agency

Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors, [redacted] Target U.S. Companies and Local U.S. Government Officials Using Voter Registration-Themed Emails, Spoof Election-Related Products and Services, Research Absentee Ballot Email Addresses; August to November 2016 (TS//SI//OC/REL TO USA, FVEY/FISA)

(U//FOUO) INTELLIGENCE PURPOSES ONLY: (U//FOUO) The information in this report is provided for intelligence purposes only but may be used to develop potential investigative leads. No information contained in this report, nor any information derived therefrom, may be used in any proceeding (whether criminal or civil), to include any trial, hearing, or other proceeding before any court, department, agency, regulatory body, or other authority of the United States without the advance approval of the Attorney General and/or the agency or department which originated the information contained in this report. These restrictions apply to any information extracted from this document and used in derivative publications or briefings.

(U//FOUO) CYBERSECURITY INFORMATION: (U//FOUO) The unclassified data in this report is protected from public disclosure by Federal Law. This report includes sensitive technical information related to computer network operations that could be used against U.S. Government information systems. Any scanning, probing, or electronic surveying of IP addresses domains, email addresses, or user names identified in this report is strictly prohibited. Information identified as UNCLASSIFIED//FOR OFFICIAL USE ONLY may be shared for cybersecurity purposes at the UNCLASSIFIED level once it is disassociated from NSA/CSS. Consult the originator prior to release of this information to any foreign government outside of the original recipients.

SUMMARY (U)

(TS//SI//OC/REL TO USA, FVEY/FISA) Russian General Staff Main Intelligence Directorate actors [redacted] executed cyber espionage operations against a named U.S. Company in August 2016, evidently to obtain information on elections-related software and hardware solutions, according to information that became available in April 2017. The actors likely used data obtained from that operation to create a new email account and launch a voter registration-themed spear-phishing campaign targeting U.S. local government organizations. The spear-phishing emails contained a Microsoft Word document trojanized with a Visual Basic script which, when opened, would spawn a PowerShell instance [redacted]

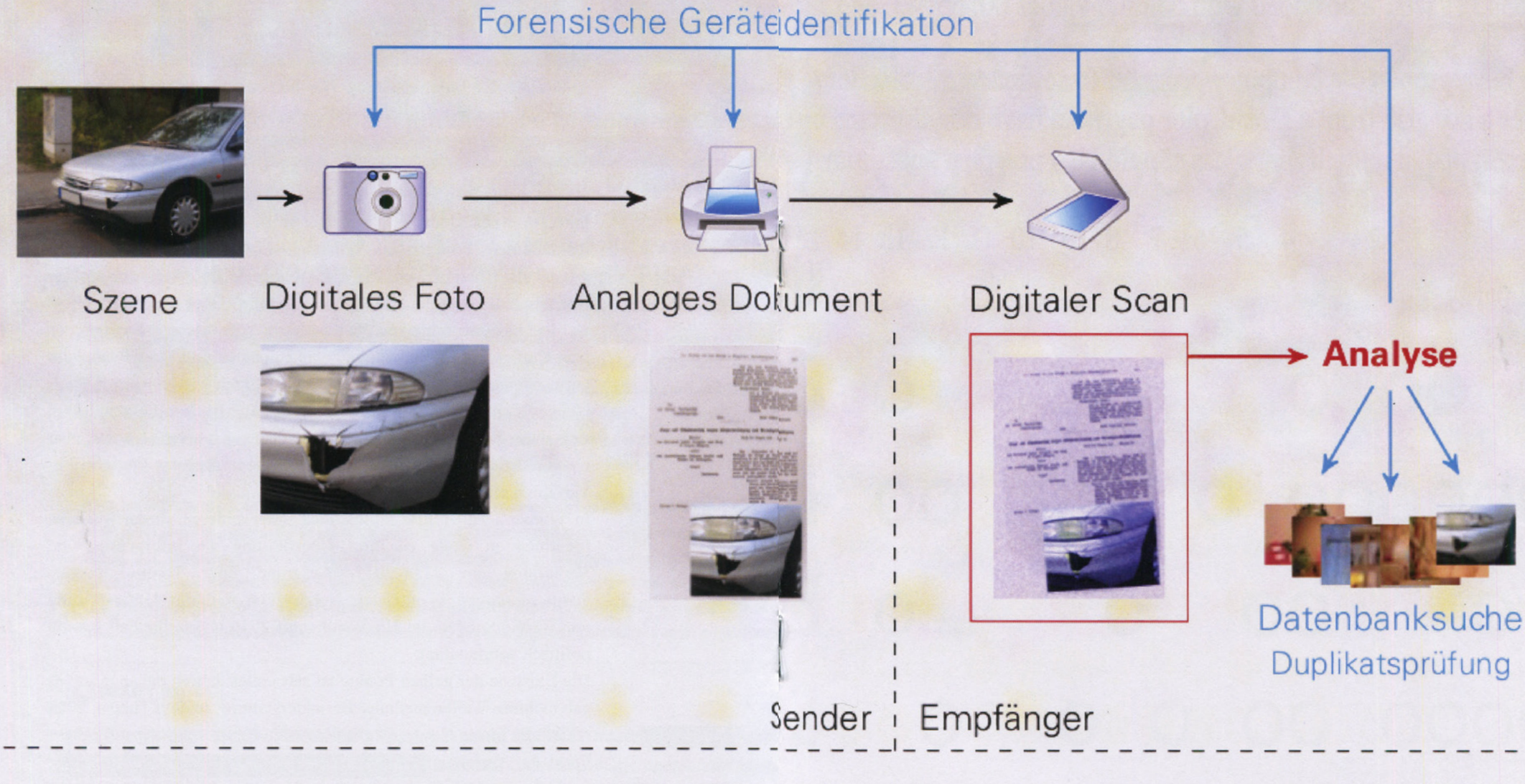
Declassify On: 20420505

Die US-amerikanische Whistleblowerin Reality Leigh Winner war bis zu ihrer Verhaftung beim NSA-Dienstleister *Pluribus International Corporation* tätig und verfügte über eine Top Secret-Freigabe. 2017 spielte sie der Internetzeitung *The Intercept* nachrichtendienstliche Informationen zur Hackeraffäre zwischen Russland und den USA ab 2016 zu. Die von ihr zugespielten Dokumente wurden von *The Intercept* als PDF-Scans der Originale veröffentlicht und enthielten einen sogenannten Machine Identification Code, den eine Vielzahl von Farblaserdruckern in Form winziger gelber Punkte in ausgedruckten Dokumenten hinterlassen. Dieses steganographische Verfahren wurde als Übereinkunft zwischen Industrie und Regierungen zur forensischen Geräteidentifikation eingeführt. Über das Blatt verteilt werden in einer winzigen Punkt-Matrix spezifische Informationen zum Kopier- bzw. Druckvorgang wie Hersteller und Modellname des verwendeten Geräts sowie Datum und Uhrzeit hinterlassen. Mittels blauem Licht, einem Mikroskop oder digitaler Bildbearbeitung lassen sich diese Markierungen sichtbar machen und beispielsweise über ein von der *Electronic Frontier Foundation* im Reverse Engineering-Verfahren entwickeltes Online-Tool entschlüsseln.

In Winner's Fall führte mutmaßlich unter anderem dieser Machine Identification Code zu ihrer Überführung als Informantin und Verhaftung am 03.06.2017. Aufgrund ihrer Trump-kritischen Positionierungen in sozialen Netzwerken und der Unterstützung von Bernie Sanders im US-Wahlkampf 2016 wurde ihr Fall schnell politisch vereinnahmt.

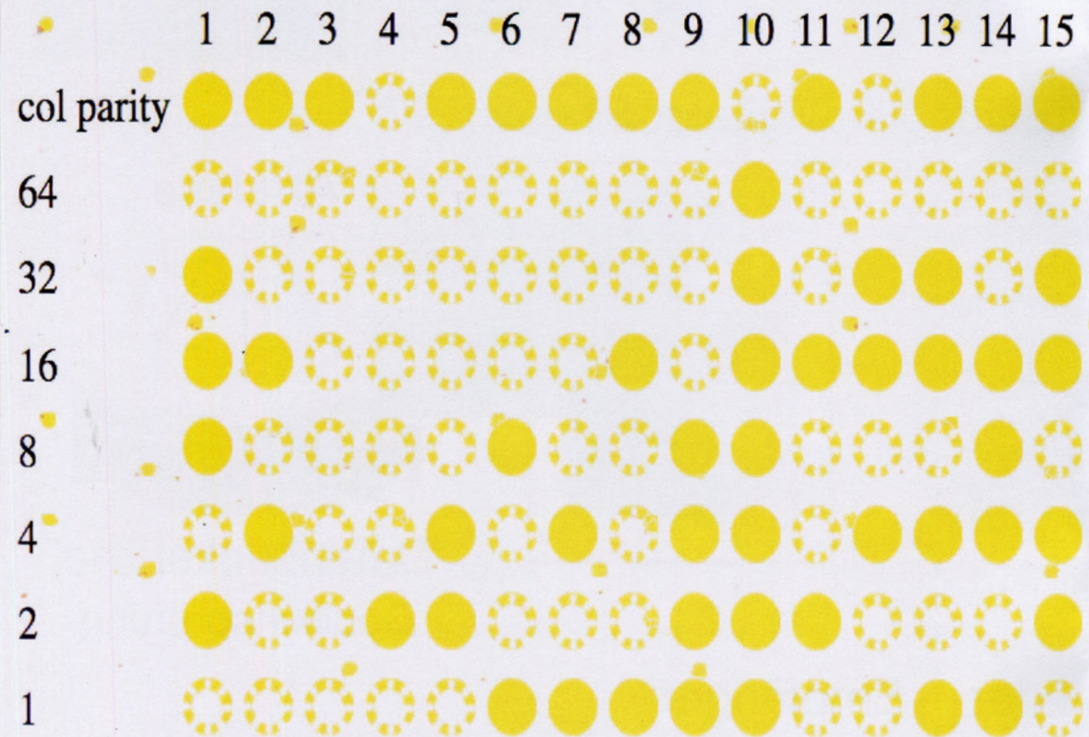
Die Existenz der gelben Punkte ist seit vielen Jahren bekannt und es gab mehrere Wellen medialer Berichterstattung zu dem Thema. 2004 erhielt die Firma *Canon Deutschland* den *BigBrotherAward* für diese Form der Verletzung von Privatsphäre. Mittlerweile weisen einige unabhängige Untersuchungen darauf hin, dass sämtliche Ausdrucke bzw. Kopien von Farblaserdruckern neuerer Bauart eine Form von Machine Identification Code enthalten, in den häufigsten Fällen gelbe Punkte. Forscher der TU Dresden konnten einen Großteil der Matrizen entschlüsseln und bieten ein Tool zum Download an, das die Lesbarkeit der Codes durch das Hinzufügen weiterer gelber Punkte beim Druckvorgang unterwandert.

Dieses Heft enthält aufgrund seiner Herstellungsweise Hinweise zu Entstehungszeitpunkt und verwendeter Technik.


Forensische Geräteidentifikation
Szene
Digitales Foto
Analoges Dokument
Digitaler Scan
Analyse
Datenbanksuche
Duplikatsprüfung
Sender
Empfänger

The printer serial number is a decimal number of six or eight digits; these digits are coded two at a time in columns 14, 13, 12, and 11 (or possibly just 13, 12, and 11); for instance, the serial number 00654321 would be coded with column values 00, 65, 43, and 21.

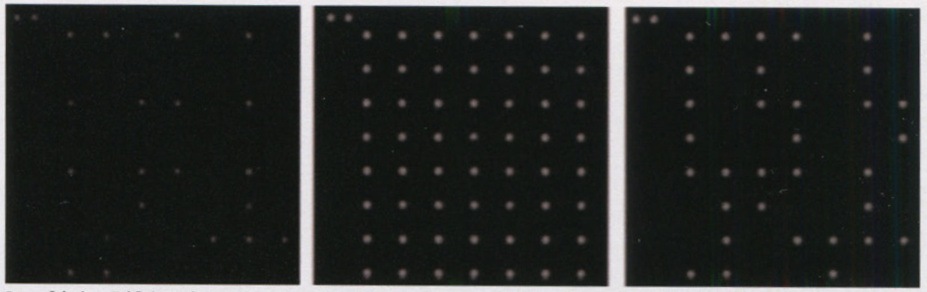
We have prepared a computer program to automate this decoding process. Below, you can interactively enter a dot grid from a DocuColor page and have it interpreted by our program. If you don't have a microscope, a magnifying glass should be a practical substitute.



EFF does not log the information submitted to this web form or the results it returns. If you prefer, you can download the source code of this program, which we have licensed under the GNU General Public License.

```
111111
123456789012345
7  ooo  ooooo  o  ooo
6              o
5  o           o  oo  o
4  oo       o  oooooo
3  o     o    oo    o
2   o   o o o  oo  oooo
1  o   oo    ooo     o
0        ooooo   oo
```

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
'''
Creates an anonymisation mask for tracking dots.
This needs to read a scan of the printed calibration page.

Copyright 2018 Timo Richter

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.
'''

import sys, cv2, argparse, json, random
import numpy as np
from colorsys import rgb_to_hsv
from libdeda.psfile import PSFile
from libdeda.print_parser import PrintParser, patternDict
from libdeda.extract_yd import rotateImage, matrix2str
try:
    import Image
except ImportError:
    from PIL import Image
from libdeda.cmyk_to_rgb import CYAN, MAGENTA, BLACK


TESTPAGE_SIZE = (8.3, 11.7) # A4, inches
EDGE_COLOUR = MAGENTA
EDGE_MARGIN = 2.0/6 # inches
MARKER_SIZE = 5/72


class Main(object):
    testpage = "testpage.ps"

    def argparser(self):
        parser = argparse.ArgumentParser(
            description='Create an anonymisation mask for tracking dots')
        group = parser.add_mutually_exclusive_group(required=True)
        group.add_argument("-w", "--write", default=False, action='store_true', help='Write calibration page to "%s"'%self.testpage)
        group.add_argument("-r", "--read", type=str, metavar='FILE', help='Read scanned calibration page and create anon mask')
        parser.add_argument("-v",'--verbose', action='count', default=0, help='Fehlerausgabe')
        self.args = parser.parse_args()

    def __init__(self):
        self.argparser()
```



Das linke Bild zeigt ein Tracking-Muster. In der Mitte sind alle Punkte in der Matrix aufgefüllt. Das rechte Bild zeigt das minimale Muster, um das Tracking unbrauchbar zu machen. – All rights reserved TU Dresden

Damit alle ihre Ausdrucke anonymisieren können, haben Timo Richter und Stephan Escher ein Toolkit entwickelt, das sie zum Herunterladen bereitstellen. „Wir finden es wichtig, dass die Menschen über die vorhandenen Codes und die damit mögliche Überwachung aufgeklärt werden“, sagt Escher. Sein Kollege Richter findet: „Jeder Mensch sollte sich frei äußern können – dazu gehört auch das Aufdecken von Missständen.“

Doch man muss nicht erst NSA-Dokumente leaken, um ein Interesse daran zu haben, anonym Dokumente drucken zu können. Als weiteres Beispiel nennen die beiden in ihrem Paper regierungskritische Flugblätter, die Aktivisten in Diktaturen verbreiten. Lässt sich ihr Drucker und damit die zugehörige Person ermitteln, stellt das eine große Gefahr für sie dar. – https://netzpolitik.org/

https://dfd.inf.tu-dresden.de/#tool

seeing yellow

(https://www.eff.org/files/filenode/printers/ccc.pdf